360数字安全

数 字 安 全 的 领 导 者

360 安全浏览器
产品白皮书

版权声明

目 录

修订记录

版本	修订时间	修订人	修订内容
V2.0	2020-7-3	郭建强	创建文档
V2.1	2021-6-1	郭建强	更新文档，如数据可视化、SDP 安全准入
V3.0	2023-9-1	郭建强	全新企业版 3.0 发布

1. 背景

在实际的企业环境中，浏览器早已成为办公场景中最常见的基础设施，用户已经习惯将打开浏览器作为电脑启动后的第一件事，通常也会在下班之前才去关闭它，可以说浏览器在潜移默化中已然与用户的工作场景融为一体。而正是这样一个与用户朝夕相伴的工具，却始终因为各种原因导致在企业办公场景中问题重重，对于员工的使用体验、企业的整体效率，以及各层面的安全性都造成了较大的影响，主要可以概括为以下几个方面：

1.1. 业务系统兼容性问题

以我国为例，随着十几年的信息化发展历程，面向企业的业务系统建设年代通常较为久远，在众多的核心业务系统中，有相当大一部分业务系统是需要依赖 IE 浏览器打开并配置相关选项后才能正常访问的，页面兼容性在工作中带来各种不同的问题现象：

- 访问的页面无法正常显示、用户无法正常登录、需要使用的插件无法正常加载和运行、各种配置参数总是被第三方软件篡改等
- 对于普通用户，因为业务系统的适配浏览器内核不同，很多时候他们不得不在同一台电脑上安装各种不同的浏览器来访问对兼容性有不同需求的业务系统
- 而插件作为浏览器能力的补充，为用户提供了更加丰富的使用场景，在很多基于 IE 浏览器开发的业务系统中，更是在诸多方面都依赖于 ActiveX 插件。大部分普通用户，对于在访问哪个系统时需要插件，使用什么功能时需要插件，以及插件如何下载安装等问题，大部分最终用户是不清楚的

1.2. 配置处理的碎片化与重复处理问题

浏览器使用过程中所产生的配置问题导致员工不得不停下手头的工作去解决这些问题，企业里的大多数员工都是面向自己业务的能手，但对于这种 IT 技能通常不会像技术人员那样得心应手，普通解决这样的浏览器相关的一个问题需要花费他们几十分钟的时间，保守举例推算一下：一个上万人的企业，假设每人花十分钟去处理一个由“未签名的 ActiveX 控件”和“Windows Defender SmartScreen”导致的 OA 系统无法正常使用的问题，那么这个企业所花费的总工作时长为： 10 分钟 * 10000 人 / 60 分钟 / 8 小时 = 208 天 纯工作时间，这是非常

巨大的资源浪费。

1.3. 访问通信安全问题

网络通信安全已上升至我们国家的战略高度，无论是互联网还是大数据及物联网时代，通信安全一直都是被关注的焦点。在中国对基础设施领域的信息安全需求之下，我国制定了自主知识产权的 ECC 国家标准算法，商用密码算法将有效保障网络信息安全。浏览器作为用户与网络信息世界的接口，是商用密码算法的重要落脚点和应用普及的关键环节，但是由于操作系统的制约和国际主流浏览器的限制，之前没有任何一款通用浏览器产品能够支持商用密码算法，这给我们国家的网银、电子商务交易、税务、电子政务等各类与民生息息相关使用场景中对于商用密码算法的应用普及造成了严重的阻碍。

1.4. 内部数据揭露的风险

从威胁猎人发布《2022 年数据资产泄露分析报告》和 Verizon（威瑞森）发布的《2023 年数据泄露调查报告》中可以看到，有 19%（Verizon 报告）和 54%（威胁猎人报告）的数据泄露是由于企业内部人员造成的，内部威胁逐渐成为数据泄露的主要原因之一。

员工的很多行为都可能会对企业安全造成危害，如页面分享、数据内容拍照、无授权打印、文本复制、恶意删除等行为都会成为数据泄露或攻击的途径。并且在通常情况下，浏览器作为高频刚需的日常办公产品，与业务系统交互过程中包括上传下载文件、渲染网页、通讯过程中的数据落地都存在数据泄露隐患：

- 比如在访问网页的过程中会在本地留下缓存数据以加快浏览速度，但通常这些数据的保存形式都是明文的，这就为攻击者留下了可乘之机，有些攻击者直接去通过窃取浏览器中留下的这些静态信息来分析出有价值的数据内容。

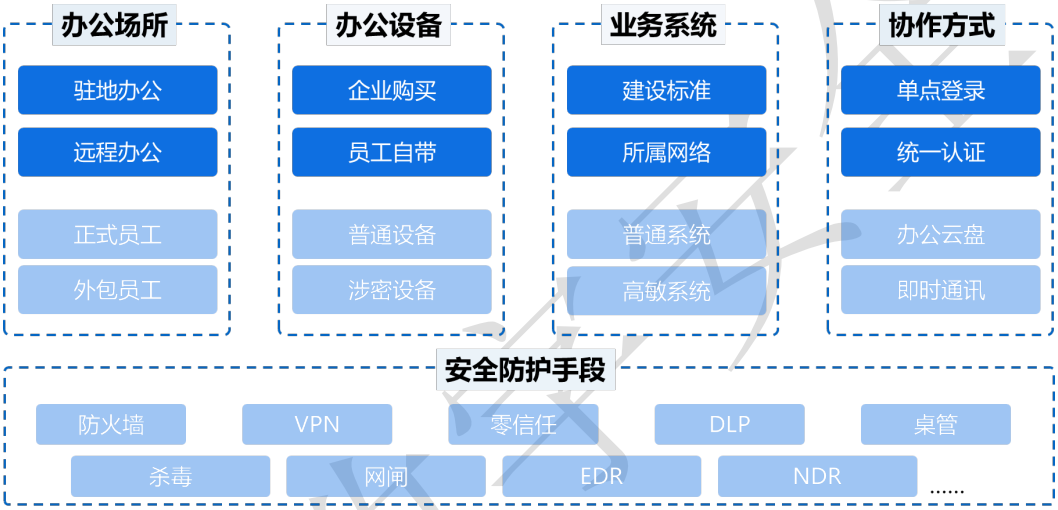
1.5. 办公场景中的安全建设盲区与死角问题

在整体安全防护体系的建设过程中，任何相关角色或领域的安全短板都可能导致整个安全体系的坍塌。现今企业的 CIO、CSO 一定在处理各种信息化建设和安全建设层面，都非常担心安全盲区和安全死角。

浏览器是用户与网络信息世界的接口，它既是用户行为的出口，又是信息数据的入口，我

们每天的工作过程中都有无数种中招的可能性，有可能因为用户安全意识薄弱，也可能是因为浏览器漏洞，导致企业终端被攻陷之后，导致企业安全建设和信息化建设的大局受到冲击。甚至说，一旦发生安全事故，无论是数据外泄还是暴力攻击，浏览器作为保护用户信息数据的安全性，便显得至关重要。越来越多的企业管理层，都逐步认识到企业级浏览器产品选型过程中，安全管控能力是一个重要考量因素。

1.6. 如何适应数字时代的终端工作安全格局



随着时下应用上云、移动办公、远程办公等场景越来越普及，新的应用接入方式与办公方式使得传统固有的安全边界被打破，无论是办公场所、办公设备、业务系统、协作方式，都发生了诸多变化，企业的终端工作格局正在从“有边界”向“无边界”进行转变。

2. 产品概述

2.1. 产品定位

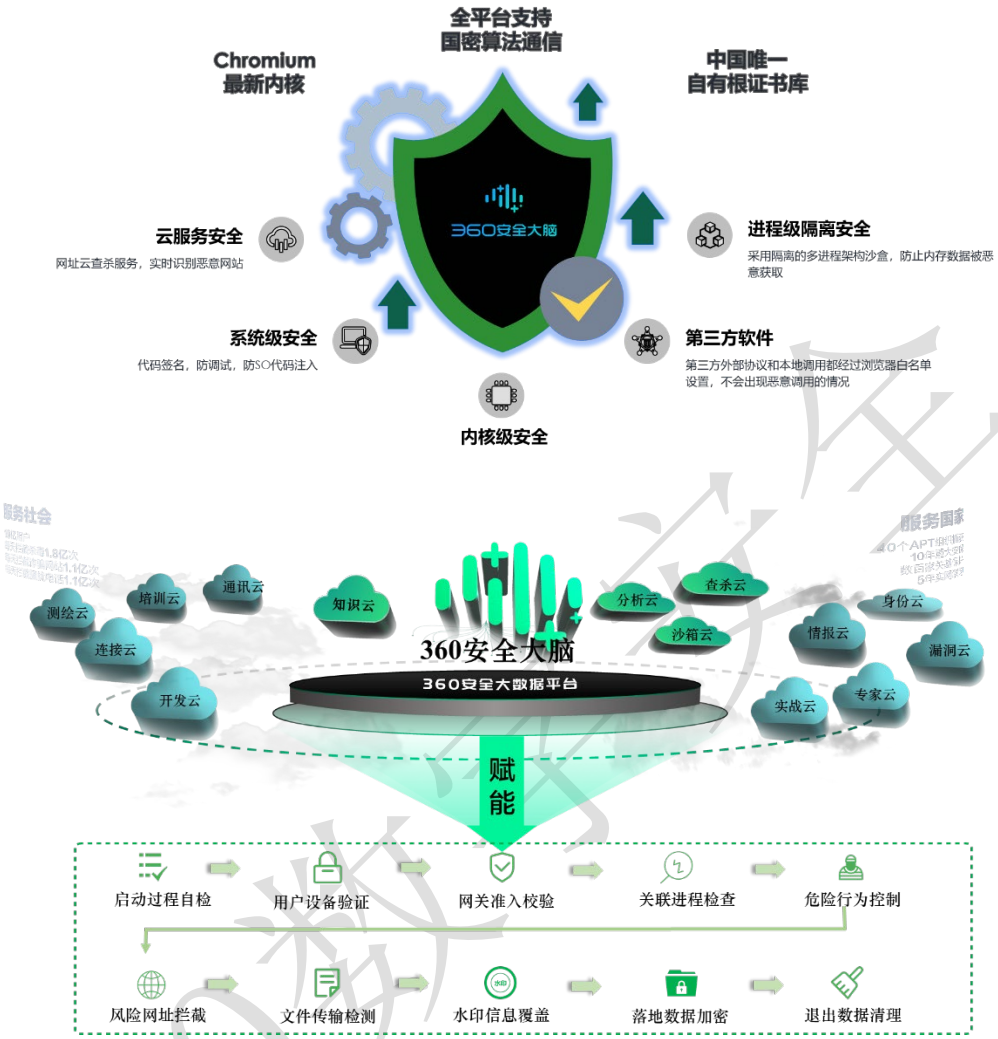
360 安全浏览器是一款以浏览器为载体，面向党、政、军、企以提高桌面工作效率、降低工作协作成本、保护企业数据安全、全平台统一场景化管控为需求目标的安全工作基础设施。

2.2. 设计方案

2.2.1. 兼容性和重复劳动解决方案

对于需要针对浏览器进行各类选项配置或编辑后才能正常访问的业务系统和正确安装控件才能使用的功能，360 安全浏览器的理念是：让专业的人做专业的事。在解决方案中将提供浏览器的服务端角色，由系统管理员在企业级浏览器的管理服务后台统一下发浏览器相关的配置选项参数，浏览器客户端将会按照各站点的配置策略进行自动化配置项设置，完全无须人工干预，从而大大减少普通用户在使用过程中的复杂程度，提高整体企业效率。

2.2.2.客户端安全解决方案



360 安全浏览器与 360 网盾、360 安全大脑相结合，为用户在使用过程中的安全提供各角度的防护机制。比如在使用浏览器访问网站过程中所产生的临时数据的安全保护方案、在需要密码输入环节的安全保护机制、在访问过程中对于恶意网站的防护机制、对于网站证书的安全审计机制、通过浏览器下载文件时的文件安全检测、浏览器所在操作系统的恶意进程监测、对于上网过程中的隐私保护机制和第三方扩展应用的安全审计等各个角度。

2.2.3.通信安全保护的解决方案

针对国密算法的高安全性要求，360 安全浏览器实现了中华人民共和国密码行业标准规定的相关算法，包括但不限于《GM/T 0003-2012 SM2 椭圆曲线公钥密码算法》、《GM/T 0004-2012 SM3 密码杂凑算法》、《GM/T 0002-2012 SM4 分组密码算法》等密码学算法，并实现 GB/T

38636-2020《信息安全技术传输层密码协议（TLCP）标准》所规定的国密 SSL 协议进行网络通信端点之间的单双向认证，以确保客户端安全可靠。

2.2.4. 企业数据安全解决方案

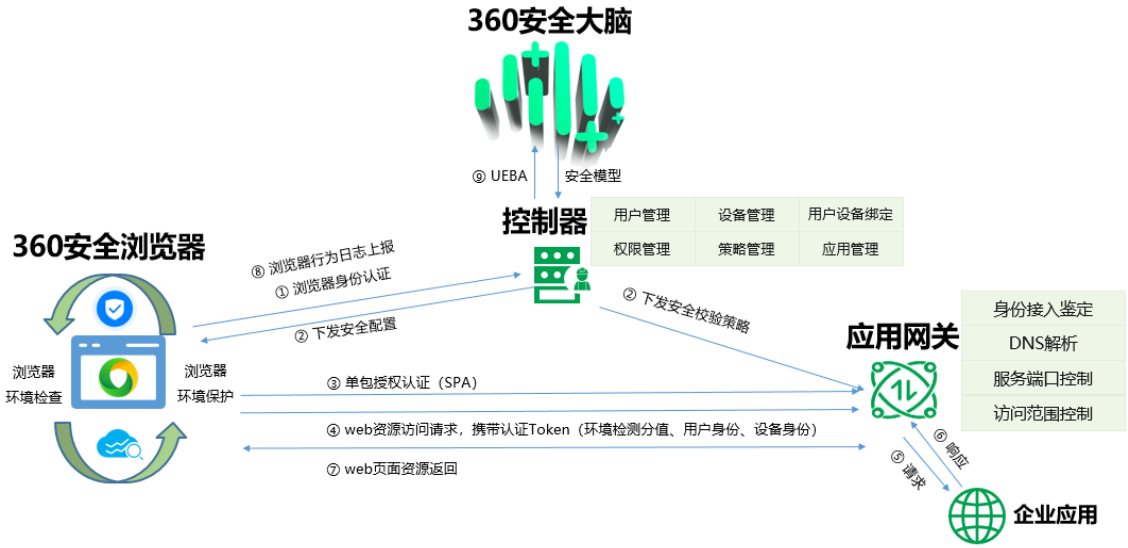
对于内部数据揭露的风险，企业管理员可以借助 360 安全浏览器作为统一的办公终端来限制不同属性的用户对于不同敏感级别的业务系统的使用权限。

- 如对于 CRM 系统，可设置禁止使用打印功能、禁止文字复制、覆盖数字水印、访问控制列表、禁用地址栏、收藏栏等一系列手段来规范员工的使用行为以及便于数据泄露的事后追责。
- 如对高敏业务系统，不允许文件下载到本地，只允许在线文件预览和编辑，实现文档不落地

2.2.5. 安全远程办公和安全准入解决方案

随着移动互联网、IoT 技术的飞速发展打破了常规的时间、空间以及设备限制，受 2020 年疫情影响，迫使大部分企业日常办公方式转向远程办公模式。传统的远程安全接入方式已经无法满足企的安全需求（不断发生的安全事件、基于 SSL 协议的远程软件漏洞频发）。企业的业务应用系统逐步迭代过程也存在安全风险，在海量的黑客面前，任何细微的漏洞都可以被利用，导致安全风险被无限放大，同时无限的接入也使得传统网络日趋疲惫。所以传统的网络安全边界已经逐模糊、甚至透明，严重危险用户的数据资产。

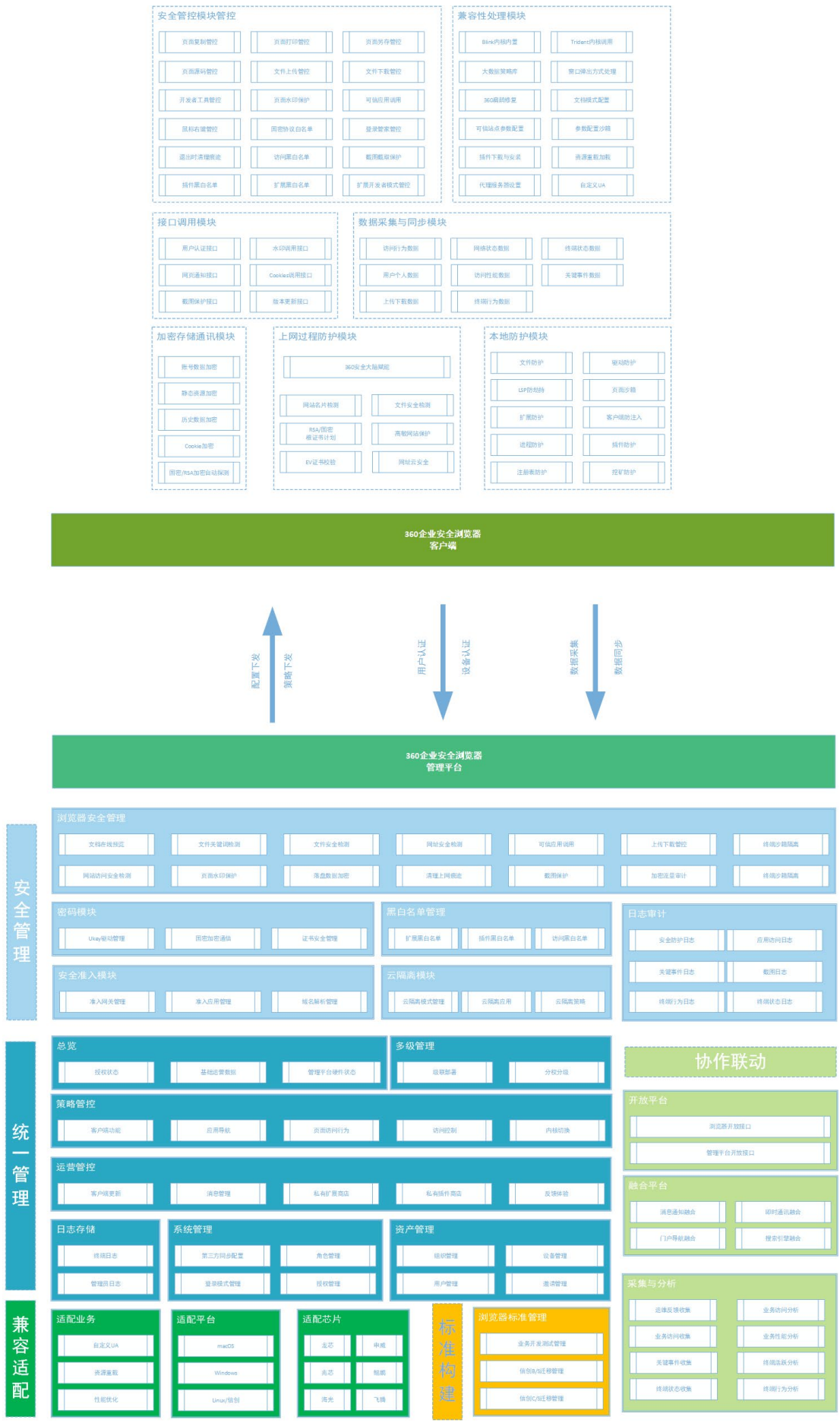
为解决以上问题，360 安全浏览器引入 CSA 安全联盟零信任架构，搭建安全、可控、轻量级的远程办公准入平台，包括三大组件：360 安全浏览器、控制器（360 安全大脑同时赋能）、应用网关，如下图所示：



- 客户端：用户通过 360 安全浏览器访问内容应用的入口，客户端集多因子身份认证、环境检查、环境保护，客户端浏览器支持 Windows、macOS、Linux、信创操作系统、Android、iOS 全平台。
- 控制器和 360 安全大脑：控制器与 360 安全大脑联动，用来对所有接入的客户端以及涉及到的网关进行管理，制定并即时下发安全策略。
- 应用网关：应用网关对客户端访问内容应用的所有数据包进行验证和过滤。

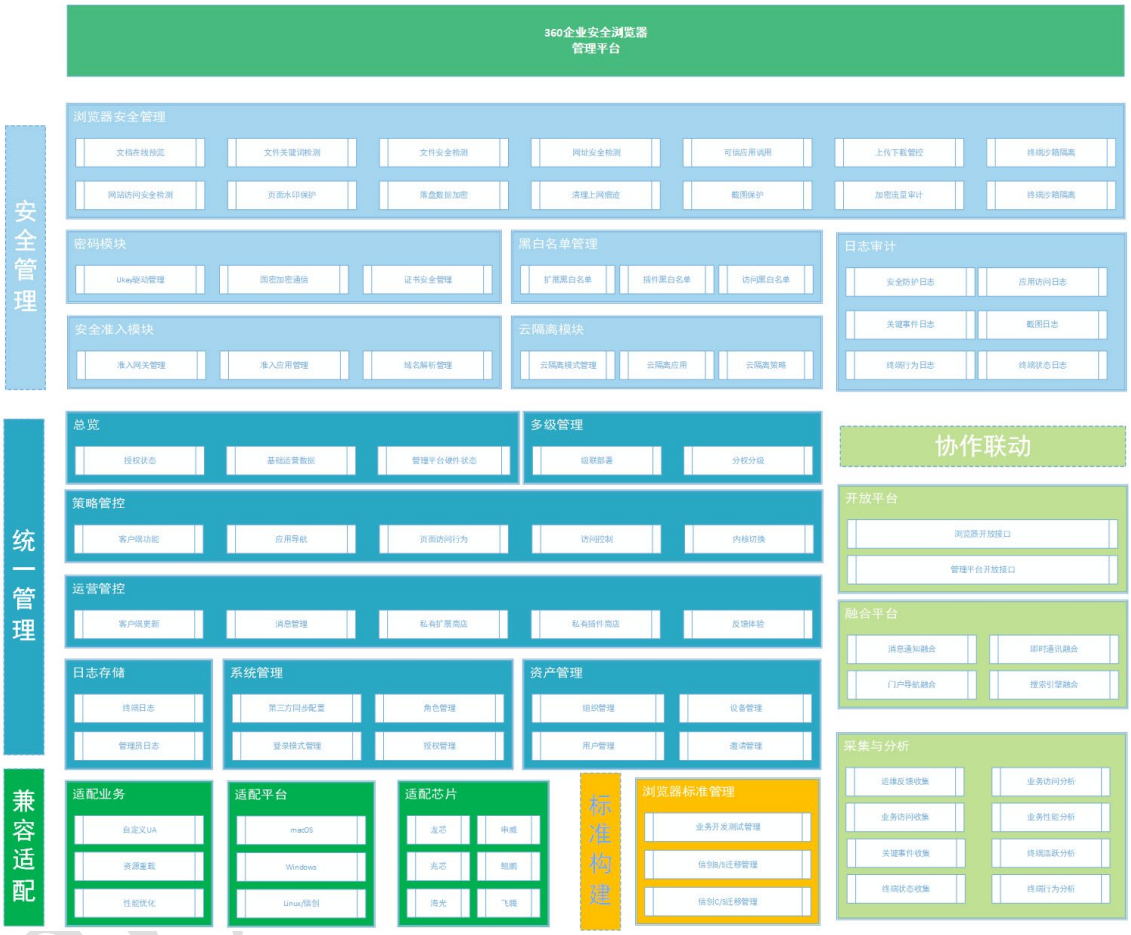
2.3. 产品架构

360 安全浏览器的产品架构如下图所示：


安全管控模块管控
页面复制管控
页面打印管控
页面另存管控
页面源码管控
文件上传管控
文件下载管控
开发者工具管控
页面水印保护
可信应用调用
鼠标右键管控
国密协议白名单
登录管家管控
退出时清理痕迹
访问黑白名单
截图截屏保护
插件黑白名单
扩展黑白名单
扩展开发者模式管控
兼容性处理模块
Blink内核内置
Trident内核调用
大数据策略库
窗口弹出方式处理
360漏洞修复
文档模式配置
可信站点参数配置
参数配置沙箱
插件下载与安装
资源重载加载
代理服务器设置
自定义UA
接口调用模块
用户认证接口
水印调用接口
网页通知接口
Cookies调用接口
截图保护接口
版本更新接口
数据采集与同步模块
访问行为数据
网络状态数据
终端状态数据
用户个人数据
访问性能数据
关键事件数据
上传下载数据
终端行为数据
加密存储通讯模块
账号数据加密
静态资源加密
历史数据加密
Cookie加密
国密/RSA加密自动探测
上网过程防护模块
360安全大脑赋能
网站名片检测
文件安全检测
RSA/国密
根证书计划
高敏网站保护
EV证书校验
网址云安全
本地防护模块
文件防护
驱动防护
LSP防劫持
页面沙箱
扩展防护
客户端防注入
进程防护
插件防护
注册表防护
挖矿防护
360企业安全浏览器
客户端
配置下发
策略下发
用户认证
设备认证
数据采集
数据同步
360企业安全浏览器
管理平台
安全管理
浏览器安全管理
文档在线预览
文件关键词检测
文件安全检测
网址安全检测
可信应用调用
上传下载管控
终端沙箱隔离
网站访问安全检测
页面水印保护
落盘数据加密
清理上网痕迹
截图保护
加密流量审计
终端沙箱隔离
密码模块
Ukey/驱动管理
国密加密通信
证书安全管理
黑白名单管理
扩展黑白名单
插件黑白名单
访问黑白名单
日志审计
安全防护日志
应用访问日志
关键事件日志
截图日志
终端行为日志
终端状态日志
安全准入模块
准入网关管理
准入应用管理
域名解析管理
云隔离模块
云隔离模式管理
云隔离应用
云隔离策略
统一管理
总览
授权状态
基础运营数据
管理平台硬件状态
多级管理
级联部署
分权分级
协作联动
策略管控
客户端功能
应用导航
页面访问行为
访问控制
内核切换
开放平台
浏览器开放接口
管理平台开放接口
运营管控
客户端更新
消息管理
私有扩展商店
私有插件商店
反馈体验
融合平台
消息通知融合
即时通讯融合
门户导航融合
搜索引擎融合
日志存储
终端日志
管理员日志
系统管理
第三方同步配置
角色管理
登录模式管理
授权管理
资产管理
组织管理
设备管理
用户管理
资源管理
采集与分析
运维反馈收集
业务访问分析
业务访问收集
业务性能分析
关键事件收集
终端流畅分析
终端状态收集
终端行为分析
兼容适配
适配业务
自定义UA
资源重载
性能优化
适配平台
macOS
Windows
Linux/信创
适配芯片
龙芯
申威
兆芯
鲲鹏
海光
飞腾
标准构建
浏览器标准管理
业务开发测试管理
信创B/S迁移管理
信创C/S迁移管理

其中管理后台提供策略和配置的统一下发、日志收集、设备认证等服务。客户端浏览器依据服务端下发的策略和配置进行使用。客户端浏览器支持 Windows、macOS、Linux、信创操作系统平台

2.3.1. 统一管理后台

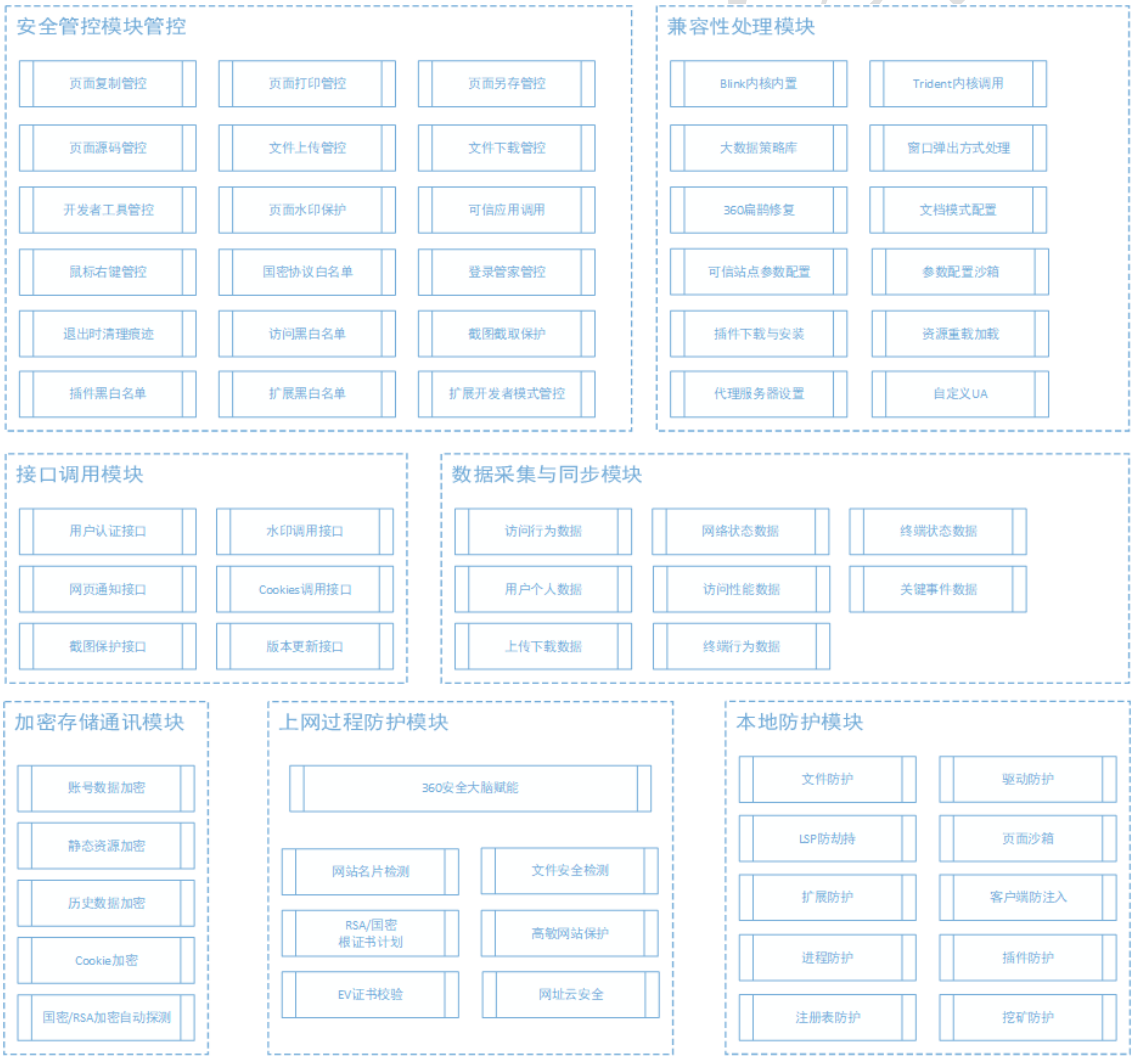


面向企业 IT 管理员提供的一套企业级浏览器集中管理控制平台：

1. 管理后台提供了包括部门及用户的组织结构管理功能，支持以组织、用户/设备为颗粒度的管控能力；
2. 管理平台具备十分强大的浏览器内核切换策略、IE 可信站点配置、弹出窗口、插件管理等功能，协助 IT 管理员处理兼容性相关的配置问题；
3. 管理平台具备对组织、用户/设备的策略管理能力，包括用户行为、访问控制、安全保护、客户端策略等维度的管控能力；
4. 管理平台具备云端扩展商店和私有化扩展商店等相关功能，协助 IT 管理员在扩展业务支撑上提供更安全便捷的功能。

5. 管理平台具备数据开放平台能力，包括但不限于对接组织/用户/设备同步、消息通知同步、待办同步等功能，让企业业务办公更加便捷高效。
6. 管理平台具备安全准入管理功能，赋能以浏览器为载体作为 Client 端，匹配企业内外部网关 Gateway 后，提供诸如单包授权认证（SPA）、用户身份认证、设备身份认证、私有 DNS 等安全准入功能。
7. 管理平台具备数据开放平台的相关功能，提供多项可协助企业数据安全输入和输出的开放接口。

2.3.2. 浏览器客户端



企业级浏览器客户端在启动后需要向管理后台提交用户/设备身份信息，以便认证自己的身份并获取相关的配置及访问策略数据；为达到企业效率最大化的目的，浏览器客户端的相关功能和能力将以管理员统一下发的相关配置策略为准，比如管理员在管理后台中设置了针

对某个业务系统禁止进行复制和打印的操作后，浏览器客户端访问到该业务系统时，会发现针对该系统相关页面的数据无法进行复制和打印，并伴随相关的提示信息。

3. 产品核心功能

3.1. 兼容适配

3.1.1. 内核自动切换（仅支持 Windows 平台）

360 安全浏览器中内置了最新版本的 Blink 内核，Blink 内核具有更高的网页浏览速度和更好网页渲染效果。但由于部分网银、政府、税务、办公系统等网站或业务系统基于 IE 浏览器进行开发或使用了 IE 特性的控件，导致其页面在 Blink 内核下无法正常显示或使用，所以 360 安全浏览器支持调用操作系统中的 IE 浏览器来模拟从 IE6 至当前 IE 版本之间的不同渲染模式。同时， 360 安全浏览器会根据系统页面 head 标签中的代码特征来判断合适的内核切换依据。

另外，360 安全浏览器、极速浏览器通过用户行为大数据积累了数十万条用户主动选择行为下产生的 host 页面和内核版本的对应关系，这些关系数据会经过 360 安全大脑的学习和判断筛选后输出到人工终验环节，运营人员通过对规则库的人为访问判断处理后，最终形成 360 智能切换策略集合 Switcher。360 安全浏览器集成了这个 Switcher 文件，当该 Switcher 判断当前系统需要特定的内核版本进行页面渲染时，便自动切换当前内核进行处理；在企业办公的

场景中，由于有些业务系统只存在于内网环境中，并没有在通用 Switcher 的覆盖范围内，针对这种情况，360 安全浏览器的管理后台向管理员开放了内核切换策略列表，允许管理员根据自己企业中业务系统的实际情况对该策略进行编辑，并将策略指令同步给浏览器客户端，当浏览器客户端访问到指定系统时，便会根据策略要求进行自动进行内核切换。

针对某些极其特殊的兼容性场景，支持单独调整打开页面的 JS 脚本解析引擎，实现页面文档渲染内核和 JS 解析引擎的分别配置。在某些特殊场景下，极大地拓展了用户针对老旧系统的集成和改造能力。

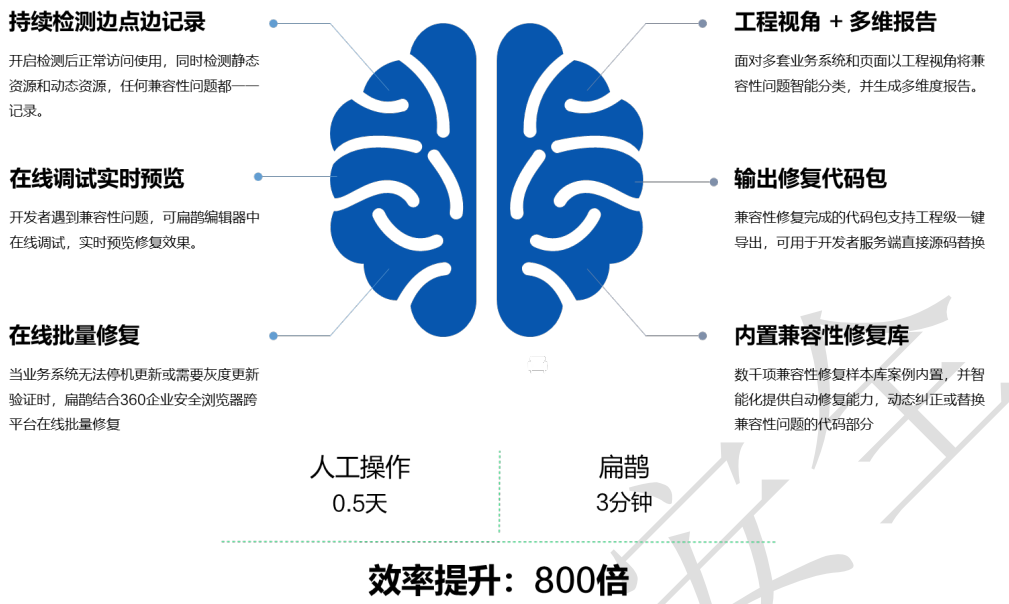
3.1.2. IE 可信站点配置（仅支持 Windows 平台）

从需求场景出发来看，企业使用 IE 的可信站点相关配置选项是为了更加顺畅的通过 IE 来访问业务系统，所以对于可信站点的安全选择通常会集中在[中]、[中低]、[低]以及[自定义]这个范围中，所以 360 安全浏览器管理后台将这部分功能配置进行了抽象，并平移到配置界面中，管理员可在后台管理界面将某些业务系统的地址加入可信站点，而且可以设置可信站点对应的安全级别，其中也包括[自定义]级别中的 52 个独立配置项。

3.1.3. 弹出窗口设置

浏览器的弹出窗口拦截功能可以帮助人们阻止网页弹出式广告和有安全威胁的弹窗，但是也可能会屏蔽那些有用的弹出窗口，因为有些业务系统的功能页面是需要通过弹出新窗口来加载和展示的。360 安全浏览器具备弹出窗口的配置功能，可以由系统管理员可以配置，在全局开启浏览器弹出窗口拦截功能的基础上，将内部需要使用弹窗才能正常工作的业务系统添加到例外网站中，从而整体解决窗口弹出的相关问题。

3.1.4. 扁鹊



我国信创产业的推进初显成效，360 浏览器团队在两年来的深度参与过程中清楚的看到，信创改造的整个过程所涉及到的内容除了整机、CPU、操作系统、办公软件等盒子里的角色以外，还有近乎无限的业务应用系统，这些系统中有很多都是基于 IE 浏览器进行开发实现的，而在信创的系统环境下，浏览器是无法使用 IE 内核的渲染能力的，这也就造成了，原来在 windows 系统上显示和交互正常的业务系统，到了信创平台上，变成了打不开、显示不了、排版错乱、交互失效等一系列问题，这时因为原来的页面不适用于 chrome 内核的解析引擎导致的兼容性问题，严重的影响了正常办公。

扁鹊是 360 浏览器推出的兼容性自动检测及修复方案，它是 360 浏览器团队经过长时间的技术积淀和探索，将技术和经验抽象成工具，帮助用户针对 web 页面进行自动化处理的技术方案。

它将 web 页面中负责展示、排版和交互的页面元素进行了分析和归类，并组合成了数百项的检测条目，通过对目标页面的自动抓取和分析，可以检测和定位到有兼容性问题的语法，当检测完毕后会通过报告的形式进行呈现，显示出目标页面中哪些部分有问题，应当怎样修复。同时，扁鹊还提供了自动化修复的能力，也就是说，这个工具会自动把页面上原来仅适合于 IE 浏览器的语法翻译成 chrome 内核支持的语法，从而可以达到正常显示的效果。非常重要的一点是，这个翻译和替换的过程都是在浏览器里完成的，不需要改造原有的业务系统。

3.1.5. 驱动适配管理

在国密加密通讯的双向认证过程中，浏览器需要通过读取 USB Key 中的证书来验证用户的身份，而浏览器需要通过加载 USB Key 的驱动才能正常识别到 USB Key 设备。但是由于缺乏统一的标准，各 USB Key 厂商对于自己设备的驱动文件存放路径是不同的，这就导致浏览器在加载 USB Key 时经常会出现驱动加载失败导致无法识别 USB key 的问题出现。

360 安全浏览器提供国密 USB Key 的驱动适配管理能力，可以将自己单位所使用的 USB Key 的驱动文件在管理界面中进行配置，从而保障浏览器启动后能够正常识别设备驱动。

3.1.6. 自定义 UA

用户代理（User Agent，简称 UA），是浏览器向网站服务器发送的一个标识，用来告诉服务器当前终端用户使用的是什么浏览器、操作系统版本、设备类型信息等。浏览器 UA 设置则是指设置或更改 UA 字符串的过程。控制用户在使用浏览器时，访问应用网站时的 UserAgent 内容，可扩展为网站的 UA 准入控制策略。

通常情况下，浏览器会默认发送自己的 UA 信息，但是有些网站会根据 UA 信息来进行判断和限制。比如，一些网站会屏蔽某些浏览器或操作系统（如早期 Linux 系统会默认 UA 为 Android 系统），或者只向特定的设备提供服务，有时，为了能够正常访问某些被限制的网站，我们需要通过修改浏览器 UA 来绕过这些限制。360 安全浏览器支持用户自己来定义 UA 中所携带的字符串内容，并可以根据需要来设置自定义 UA 的影响范围，从而规避那些由于网站判断失误所导致的页面返回样式不正常的问题。

3.1.7. 资源文件替换与 JS 脚本加载

针对一些特殊的可能存在兼容性问题的资源文件，在一些老旧应用中使用了一些兼容性不佳的脚本方法或样式方法，在显示时，可能存在无论如何调整文档模式和 JS 引擎都无法解决兼容性问题的情况，360 安全浏览器为了拓展兼容性支持边界，在处理这些特殊情况时，提出直接对存在兼容性问题的文件进行替换处理的方式，这样既避免了修改应用可能带来的额外风险，又能对兼容性问题进行额外处理。例如 js 脚本文件、css 文档样式表等文件，支持对特定文件定向替换的，直接从源头解决某些文件的不兼容问题。

一些过时的业务系统应用可能存在一些不能被正确执行的页面内容，由于存在的数量过多或出问题的资源本身就是动态资源，进行资源替换的形式进行修改可能存在修改比较复杂的情况。通常这种情况可以通过统一的执行一次页面脚本的形式进行纠正。360 安全浏览器支持针对某些指定页面在加载完成后执行一次指定的 JS 脚本，以程序化的方式自动大批量解决页面上可能存在的兼容性问题，保证页面的正常渲染。

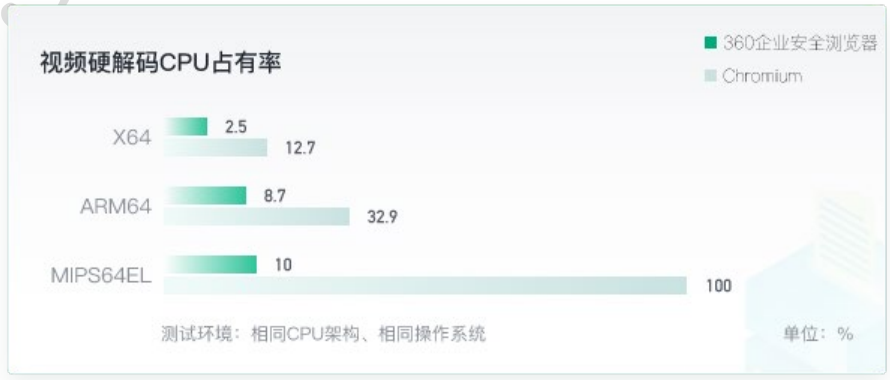
同时结合 360 扁鹊的相关能力，将原本是在一台电脑的浏览器上产生兼容性修复效果，对整个政企单位生效，企业级浏览器管理后台资源替换功能可以把 360 扁鹊的修复策略上传到管理后台进行统一的下发，所有接受到该策略的浏览器都会在访问目标页面时执行策略中的一系列修复动作，从而完成批量化的修复过程。

3.1.8. 性能优化

360 安全浏览器在 Chromium 内核基础上对性能进行了深度优化。

- 全面支持通用 GPU、国产 GPU 提供的硬件加速能力，提升渲染速度

- 全面支持通用 GPU、国产 GPU 提供的视频硬解码能力， 提升图形性能



- 全面支持国产 CPU 提供的硬件加解密能力，提升国密通信加解密速度

- 优化 FFMPEG 视频处理能力，提升高清视频浏览体验

- 优化浏览器内存保护，减少浏览使用过程中内存消耗
- 优化浏览器耗能机制，减少浏览使用过程中电能消耗

3.1.9.跨平台统一支持

360 安全浏览器全面跨平台支持，Windows 全系列（WinXP、Win7、Win8、Win10）、MacOS 全系列，尤其是支持信创全系列操作系统，如统信 UOS、银河麒麟、中科方德、Deepin、万里红、凝思磐石、中标麒麟、鸿蒙等。在信创平台的应用级产品层面，360 安全浏览器与国内各类应用厂商如插件类、签章类、输入法、服务器审计、打印刻录审计、邮件、杀毒类、电子文档类、数据库等 200 多家厂商实现全面应用兼容效果。同时，在信创操作系统上也支持了 GB/T 38636-2020《信息安全技术传输层密码协议（TLCP）标准》所规定的国密 SSL 协议进行网络通信端点之间的单、双向认证。

3.2. 统一高效管理

3.2.1.精细化、维度组合管控

支持以部门为单位的组织结构管理，支持管理员手动添加部门组织和用户，从模板批量导入部门和用户，并可以对部门及人员信息进行增删改查操作，也可以针对用户进行部门调整操作。

支持以设备为管控颗粒的管理，允许管理员手动添加设备，从模板批量导入设备，并可设置某组织部门下自动归属 IP 规则的设备，方便提前进行策略设定。

同时支持设备登录模式和账号登录模式，覆盖企业免登录使用浏览器和以企业的身份认证体系登录账号使用浏览器的双重场景。

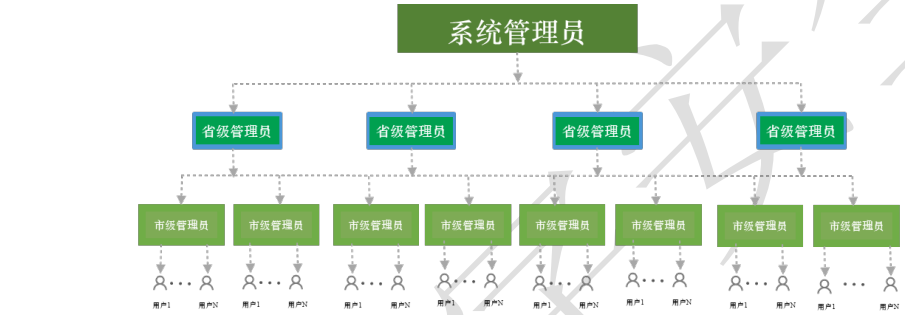
浏览器管理平台提供了诸多对接方式和接口配置能力，包括但不限于协议类（Ldap、Oauth、Saml、Cas、Radius、OpenID 等）、产品类（竹云、蓝信、Authing、吉大正元等），而且还支持企业内部自开发认证通道的配置化对接。

补图图

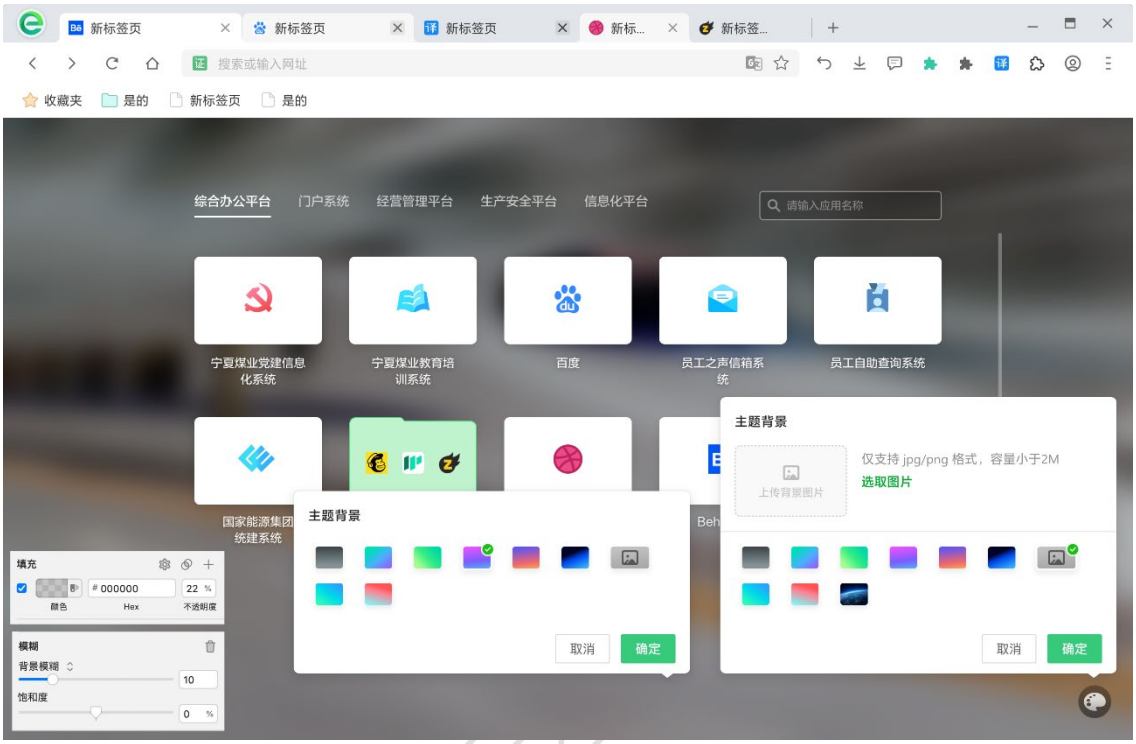
3.2.2. 分权分级管理

支持设定任意用户为角色管理员，在创建好角色管理员后，可设定某用户为该角色管理员，赋予其可以登录管理平台进行管控的能力，赋予权限包括功能权限和组织用户管理权限；角色管理员支持多层级管控，用于中大型企业的分权分级管控诉求。

权限管理支持多级管理设置，超级管理员可以设定内部管理员，分配不同的权限，内部管理员管理不同的模块，只能操作有权限的模块；超级管理员可查看管理员的详细操作日志，了解内部管理员的各项操作。



3.2.3. 统一办公入口



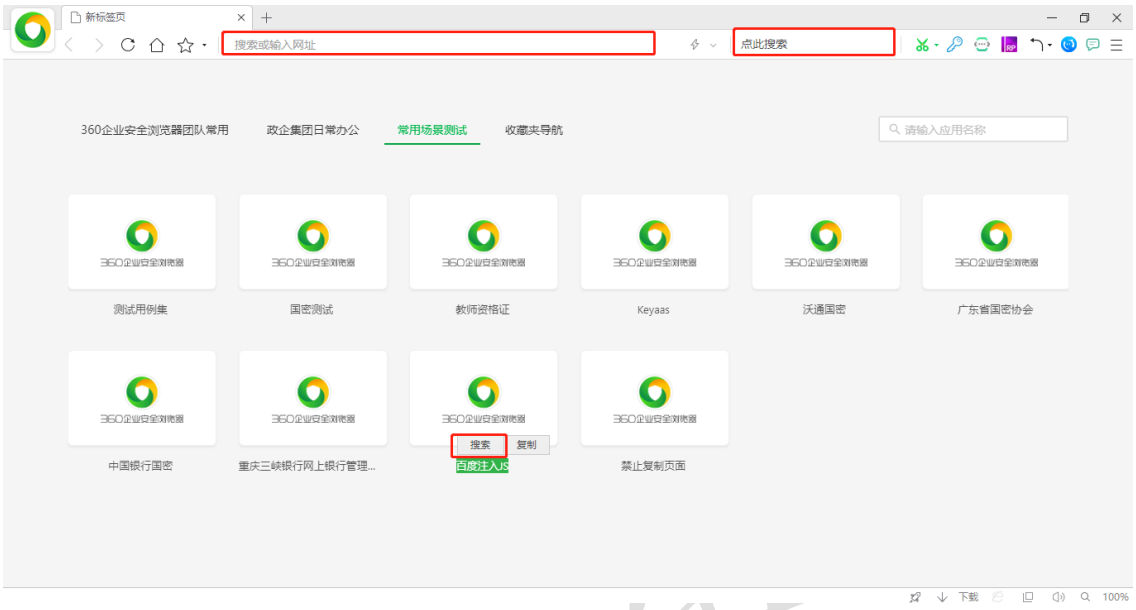
浏览器作为办公场景中用户和业务的交互出入口，每天都要去访问不同的应用系统，为了方便快捷的访问，有些用户通常会将经常访问的网站地址放进收藏夹里，那么在企业办公环境中，有没有更加统一便捷的解决方案呢？比如我们可以通过企业级浏览器为员工提供企业应用导航的服务，员工只要登录到企业级浏览器上，便可以直接看到各种应用系统，点击应用系统图标便可以直接访问到具体的业务应用。

360 安全浏览器支持由企业管理员在管理后台添加企业需要经常访问的应用信息，包括应用名称、URL 地址、图标等信息，并支持按照应用场景进行分组，而这些被添加的应用会统一下发到浏览器客户端，展示在浏览器的新标签中。应用导航策略同样支持按组织分发至客户端，用户点击图标便可以直接访问对应的业务应用系统，所属不同组织的客户端可以支持配置不同的应用导航页面。

同时支持对接企业内部的业务系统接口，将 OA、CRM 等系统消息通知、待办等信息推送到每一个用户的浏览器主页。

注：如有需求，请联系 360 安全浏览器团队获取《新标签页开放文档》

3.2.4. 搜索引擎统一



众所周知，浏览器在使用过程中可能会大量使用例如 360 好搜、百度等搜索引擎，通过搜索引擎获取所需信息。但同样是由于商业利益等原因，搜索引擎厂商存在着获取用户隐私等问题。在办公过程中不当使用搜索引擎存在着暴露组织工作内容的风险。

而且在一些企业中，拥有自行组建的内部知识库或内部搜索引擎，IT 部门希望普通用户在使用浏览器的过程中能更方便的调用这些内部信息。

为此，360 安全浏览器提供**地址栏、搜索栏、页面划词搜索**位置的搜索引擎统一功能，可灵活配置每个位置是否允许搜索引擎触发。

3.2.5. 客户端统一升级

在企业级浏览器的私有部署场景中，由于企业的管理要求、网络环境的限制以及浏览器客户端的定制化需求等原因，需要支持企业 IT 管理员通过企业级浏览器管理后台来统一处理企业中的浏览器客户端升级需求。360 安全浏览器支持将浏览器客户端安装包在管理后台进行维护，客户端定时获取配置策略的时候，获取到的该功能的相关信息；同时，客户端在本地维护一份客户端当前版本信息，并与从管理后台获取到的客户端版本信息进行比对，如果达到更新条件，则根据配置信息中的 URL 进行下载并执行覆盖安装。

- 更新范围支持按全局或按组织、按操作系统平台进行客户端更新推送；
- 更新流量支持本地流量分发推送、外部链接流量分发推送；
- 更新方式支持全量更新和增量更新；
- 更新提醒支持静默更新和提示更新；

3.2.6. 插件和扩展集中管理管控

管理平台为管理员提供插件文件管理功能，让其可以针对没有包含进浏览器安装包的第三方插件安装文件在管理平台上传并设置相关安装策略，比如浏览器客户端可以在浏览到目标业务系统时根据实际情况判断该文件是否下载并安装过，如果判断为新的插件文件，则提示用户该插件可进行下载安装，用户确认后浏览器将从后台下载该文件并执行打开动作，后续安装动作则由插件文件自行完成。

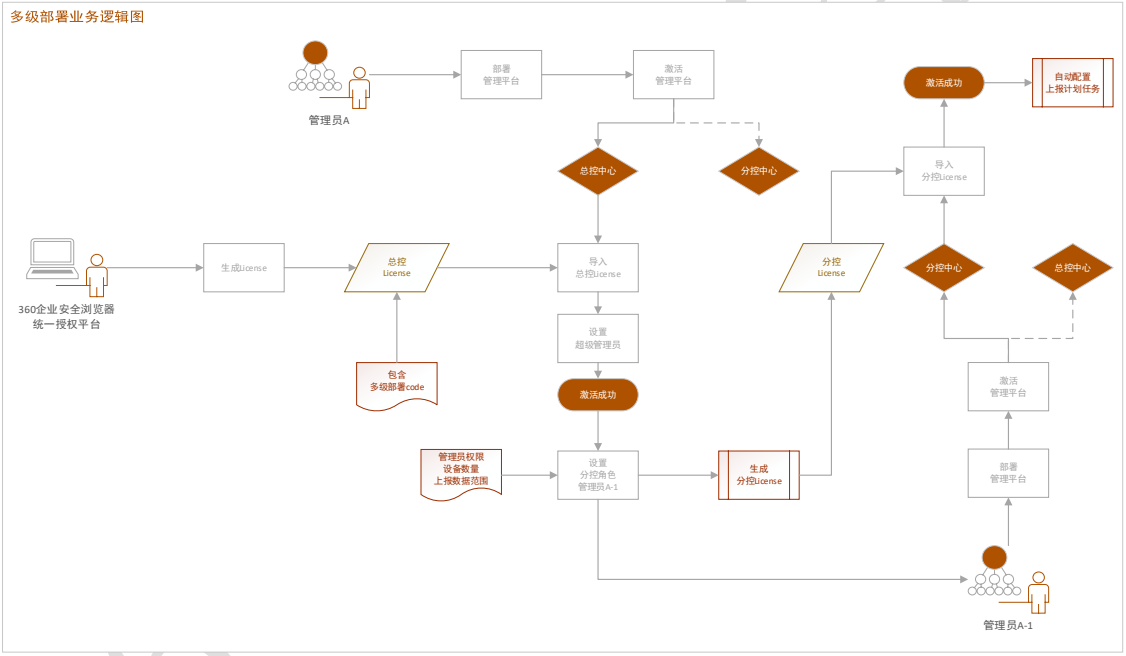
目前插件管理支持全平台全类型插件的统一管理，并支持通过版本号比对更新的功能。

管理员可以预置扩展与禁用扩展，统一管理用户的扩展；预置的扩展用户可以直接使用，禁用的扩展用户无法添加。同时还支持管控扩展在浏览器获取到的接口能力。

3.2.7. 多级级联部署管理

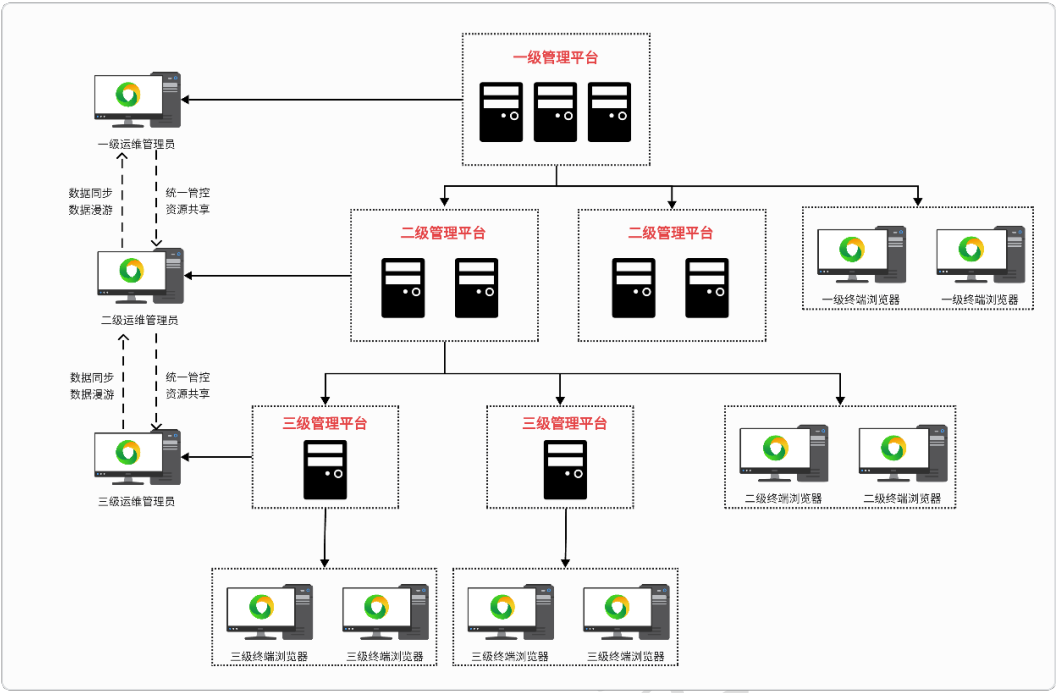
360 安全浏览器支持多种部署方式，包括单机部署、分布式集群部署、分布式多级级联部署。当企业规模变大之后，必然会面临业务系统多地分级管理的场景需求，借此 360 安全浏览器推出满足中大型企业的多级级联部署和管理的功能。

- 一套平台、自主级联



多级部署业务逻辑

由总控管理员根据配置选择是否设定分控中心，分控中心在部署完管理平台后，导入分控 License 则会自动与总控中心进行注册并联连接。



多级部署业务管理方案

- 统一管控，自主运营

各级管理平台自主运维运行管理，总控中心可设置分控中心、本地中心的相关配置和数据上报策略。

浏览器策略方案		
策略项	策略内容	备注
应用管理	可配置应用导航或者默认首页访问网址	
兼容策略	可将不同网站配置在不同的浏览器内核模式下，实现多业务系统运行于同一浏览器之上的目标。	
安全策略	可按需进行用户行为、访问控制、安全保护、客户端等安全策略的配置	
浏览器更新	可设置客户端更新版本、更新目的、更新范围、更新方式。	
证书下发	可针对内网 HTTPS 网站下发根证书，同时支持 RSA 和国密证书	
策略拉取周期	可配置客户端策略缓存有效期和获取周期	

日志存储	可配置日志存储时长	
客户端推广	可配置发布浏览器下载安装文案和链接。	

- 升级服务器部署管理

根据中大型企业升级服务应用场景中，360 安全浏览器可自由配置升级服务器，缓解企业局域网络中分发升级数据的压力，更新和分发自主可控。同时能够管理当前企业内部的版本分布情况，即使统计及通知相关终端进行升级，以确保兼容性、稳定性、安全性。

3.3. 安全防护

3.3.1. 客户端的安全保护

- 浏览器自身安全：能根据应用的特点，分别提供系统安全、进程安全、内核安全、账户安全、内容安全和应用与服务安全等安全能力。
- 浏览器系统安全：采用多进程架构，网页、代码、插件、扩展、GPU 等进程相互隔离。
- 浏览器进程安全：利用已有的沙箱机制，对沙箱里的应用进行控制，用户无论的输入是什么，沙箱都能最终确决定能做什么或不能做什么。
- 浏览器内核安全：内核脚本引擎应用能将不同的页面和扩展运行在不同的隔离域，从而保证它们不会相互访问和污染，不同隔离域的脚本不能互相访问、非同源的脚本上下文之间不能互相访问，能够自动识别 XSS 攻击代码，并对该请求进行屏蔽。
- 浏览器账户安全：具备受限访问的账户安全机制，需要实名登录才能使用，登录后浏览器必须安装有监管和审计的扩展才可以激活，通过浏览器浏敏感信息需要授权才能查看。
- 数据安全：包括访问历史，收藏，缓存，Cookie 等和用户浏览状态历史相关的数据。为了防止用户数据被其他应用篡改甚至拷贝，浏览器针对一些用户的隐私数据进行保护，比如 Cookie 信息、历史记录、保存到本地的表单密码、用户收藏的网址等等，这些数据在本地采用对称加密算法，这些算法用到的密钥一般都采用特殊算法保存在本机，可以实现即使隐私数据被盗取的情况下，没有可信硬件也是无法解密并读取其内容的。
- 安全键盘：为保护用户账号密码安全，360 安全浏览器会在指定网页的密码输入框后

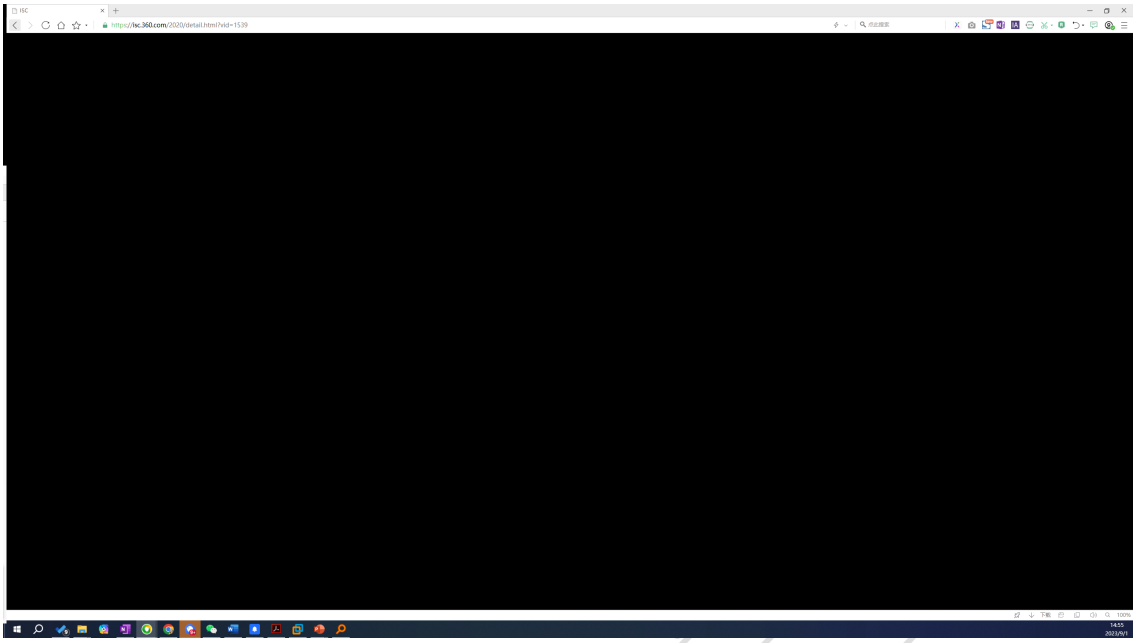
出现“安全键盘”图标，用户可通过此图标调起浏览器自带虚拟软键盘，通过软键盘进行密码输入。360 不会记录该密码信息，只是帮助用户避免被键盘记录器等硬件设备记录键盘输入，防止账号被盗财产受损。

- 网址云安全：当用户访问网站和点击网页中的链接时，本软件会对网址特征与 360 云安全计算中心的恶意网址库进行比对。当用户访问木马网站、欺诈网站时，其在地址栏会显示“危险网站”、“风险网站”等信息，同时弹出警示窗口或者跳转到警示页面，避免用户因为访问这类网站而造成的损失。
- 网站名片：当用户访问网站和点击网页中的链接时，本软件会对网址特征与 360 云安全计算中心的恶意网址库进行比对。对用户经常访问的网址、交易类、银行支付类等的官方网站进行认证，并在地址栏显示该网站的认证信息。通过对网址中的 Host 信息上传 360 的服务器进行查询可以获取该 Host 对应的网站相关信息并显示在地址栏处的网站名片中。此功能可以使用户清楚、方便地辨别该网站是否官方网站，从而避免因为访问假冒的欺诈网站受骗。当访问的网站是木马网站或者欺诈网站时，该名片显示“危险网站”并自动拦截，避免因为访问这类网站造成损失。
- 下载云安全：其依托 360 安全中心强大的“云安全技术”，下载前即可鉴定问这类网站造成损失。文件是否安全；即使已开始下载危险文件，云鉴定后也会立即阻止。

3.3.2. 安全管控策略

管理员可通过创建用户行为管控策略以及数据保护策略达到保护重要业务系统的目的。分别在用户行为和安全防护层面，配置安全管控策略。

用户行为策略可以限制用户在访问全局网站或指定网站中对相关动作的禁止与允许，全方位保护企业的内部数据资产；如截图保护



安全防护策略则可以限制用户访问在全局网站或指定网站中，增加相关围绕安全功能的启用和独立配置，防止用户或其他软件通过浏览器泄漏或窃取企业内部数据。

安全策略类型	策略内容（举例）
用户行为	禁止网页复制
	禁止网页打印
	禁止网页另存为
	禁止调用开发者工具
	禁止鼠标右键
	禁止查看页面源码
	禁止文件上传
	禁止文件下载
安全保护	页面水印
	网址云安全
	文件安全检测
	高敏网站访问安全
	清除上网痕迹
	截图保护
	国密 SSL 协议
	文档在线预览
	可信应用调用
	客户端落盘数据加密存储
	文件关键词检测
	开启“禁止跟踪(DNT)”功能

3.3.3. 国密通信功能

360 安全浏览器在产品中增加商用密码算法模块和国产安全协议模块，让浏览器所支持的双核（Chrome 和 IE）都具备国密通信的能力。同时，管理员可以按照组织/用户/设备颗粒度，在后台配置开启国密通信算法能力，开启该功能后，浏览器可以自动探测目标网站是否支持国密加通信机制，如果支持则将通信方式自动切换至国密，也可以设置目标网站在访问时只使用国密通信协议（国密 SSL 协议白名单），在普通用户无感知的前提下，有效的保障了信息通信的安全。

3.3.4. 证书管理与下发

当前 Web 页面在访问过程中，HTTPS 协议需要验证 Web 服务提供方的证书。如果证书不再客户端信任列表中，浏览器中会提示证书不可信，需要确认后才能继续访问。在国内相当多的政府机关、企事业单位中，大量使用自签证书进行服务端进行认证，由于自签证书不在系统自带的可信证书列表中，导致所有用户在进行访问时都需要进行确认后才能访问。而根证书的导入过程对于一般用户来说相对繁杂。360 安全浏览器针对这些情况，提供了从管理端下发服务端证书直接加入客户端证书信任列表的功能，该功能不仅能下发国际标准的 RSA 证书，同样可以下发国家商密证书。对于浏览器客户端的用户来说，该过程完全是透明的，客户端接受服务端策略后，访问使用自签证书的网站完全不会提示有异常提示。

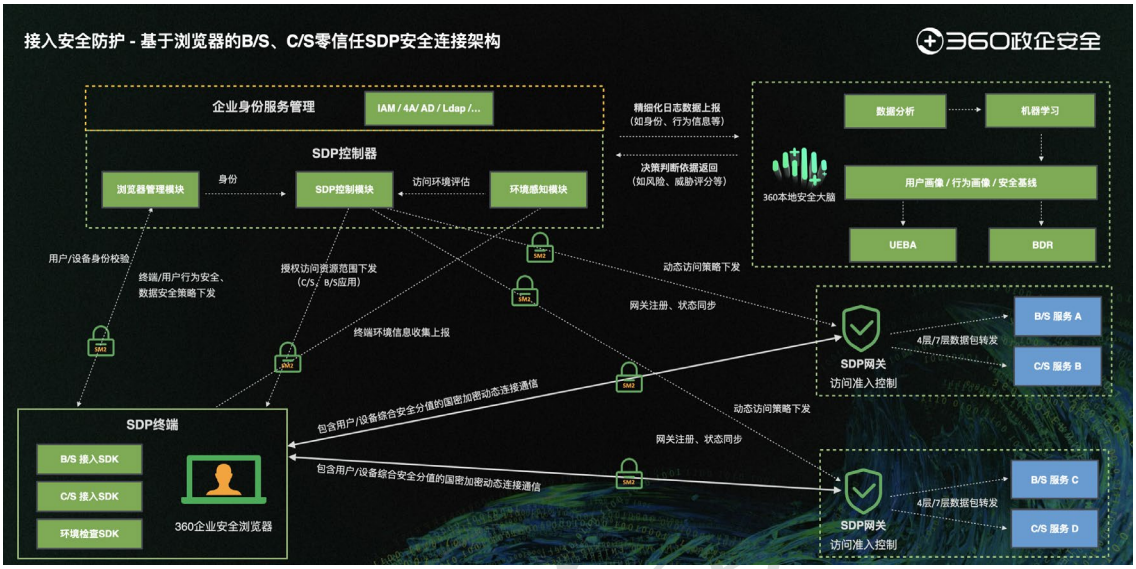
目前管理平台支持国密根证书、RSA 根证书、国密服务器证书、RSA 服务器证书的批量配置和下发。

3.3.5. 零信任安全准入管理

企业客户希望采用 360 安全浏览器来实现办公浏览器终端的统一管控，但是面临的一个挑战是，如果普通用户使用了除 360 安全浏览器之外的其他浏览器产品，那么这个用户是不在统一浏览器办公终端管控范围的。

基于这种情况，360 与市面上的应用网关产品提供商进行了沟通与协作，因为应用网关的部署位置是在所有业务应用的前面，是一个 web 反向代理的角色，生产环境中所有的访问请求都会经过应用网关进行分发。360 安全浏览器支持与已经部署在企业内部的应用网关产品进行对接及联调，通过建立浏览器客户端与应用网关之间的私有协议或者由浏览器发送请求

数据时携带特定的校验信息等方式，来实现浏览器在企业内部的排他性目的，因为普通用户通过其他浏览器访问内部业务应用系统时，不会包含相应的验证信息，自然也就无法通过应用网关的校验审核。



360 安全浏览器引入 CSA 安全联盟零信任架构，搭建安全、可控、轻量级的远程办公准入平台，包括三大组件：360 安全浏览器、控制器（360 安全大脑同时赋能）、应用网关。

基于浏览器 B/S、C/S 的零信任安全准入核心功能：

- 连接方式：先验证，后连接；
- 信息隐藏：隐藏 DNS 信息、关闭端口，扫描无法发现目标系统；
- 预认证：在访问链接请求之前先认证用户及设备的身份信息；
- 预授权：用户只能访问对其授权的业务应用范围；
- 应用层接入：只提供用户-业务的连接，只允许用户通过应用层（非网络层）访问
- 单包授权（SPA）：应用网关用来实现针对客户端访问的应用系统的数据进行转发，在转发前会对客户端进行认证，默认拒绝一切连接。验证过程中应用网关不会开放任何端口，客户端发起 UDP 数据包进行认证，数据包包括身份信息及请求开放的端口，且数据包为加密状态，应用网关不会对该数据包做响应，但会通过网关网卡的日志查看该数据包信息身份信息是否合法，权限是否正常，如应用网关验证通过后，才会允许建立转发连接。
- 国密通讯：符合国产密码和国密改造相关要求，客户端实现国密 SSL 协议双向认证。
- 私有 DNS 解析：用户在通过客户端访问业务系统时，应用网关会对访问的业务系统地址进行私有 DNS 解析。

- 客户端环境检测和保护：基于 360 安全大脑的赋能，在浏览器启动和使用过程中，可以时刻根据策略对客户端环境进行评分评估，每当发现客户端环境的评分降低或存在危险进程时，在安全准入网关的身份认证或设备认证过程，即可阻断通信来保护业务安全。
- 用户行为预警：浏览器客户端用户的 UEBA 与 360 安全大脑的强大能力结合后，将浏览器客户端的用户行为分析与 360 安全大脑（本脑）进行联动建模，当浏览器客户端的用户行为与模型基线发生偏差时，即时告警预警提醒运维管理员进行关注，也可设置相应策略进行阻断通信或暂时禁用用户。

3.3.6. 云隔离访问

360 云隔离平台以 RBI 的技术原理，独创 SNRS 智能网络渲染服务（Smart Network Render Service）将用户访问网页的全部操作，智能隔离至云容器中执行，用户通过实时镜像与云容器中的页面交互，防止任何基于 Web 攻击影响到真实用户的终端环境。

浏览器隔离技术通过将加载网页的过程与显示网页的用户设备分开，来保持浏览活动的安全。如此一来，潜在的恶意网页代码就不会在用户的设备上运行，防止恶意软件感染和其他网络攻击对用户设备和内部网络的影响。访问网站和使用 Web 应用程序涉及到 Web 浏览器从不受信任的远程来源（如遥远的 Web 服务器）加载内容和代码，然后在用户的设备上执行这些代码。从安全角度来看，这使得浏览 Web 成为一种相当危险的活动。与之相反，浏览器隔离技术能支持在远离用户的地方加载和执行代码，使他们和所连接的网络免受风险的影响。

360 云隔离平台以极具创新性的浏览器隔离技术和诸多行业首创功能，为用户提供终极 Web 安全防护和跨平台桌面应用交互，是安全隔离防护、信创迁移替代、企业数据安全保护场景中的最佳选择。主要特性如下：

- 智能隔离-B/S 应用（保护关键 web 服务免受攻击）

1. 阻断自动化攻击和扫描
   ① 隐藏 web 业务系统原始代码，阻止自动化分析和扫描；
   ② web 业务系统隐藏在云隔离平台之后，完全隔离攻击流量；
   ③ 启用客户端身份验证，仅允许受信设备访问。
2. 阻断数据泄漏
   ① 可根据安全策略设定禁止文件的上传下载；
   ② 可根据安全策略禁止对网页的内容复制、无授权打印、工具调试等；
   ③ 可根据安全策略对目标页面添加包含操作者相关信息的数字水印。
3. 安全审计
   ① 可根据安全策略对当前操作者的登录、网页访问、操作行为进行日志审计；
   ② 可根据安全策略对当前操作者的全生命周期操作行为进行录屏审计。

- 智能隔离-C/S 应用

1. 隔离 C/S 应用到云端一次性安全容器中，使用完毕立即回收，避免来自 C/S 应用的漏洞利用渗透到本地设备；
2. 浏览器在本地镜像 C/S 应用的窗口显示效果，窗口状态保持同步；
3. 支持所有 windows 平台的应用生态，覆盖文档编辑、图形图像、设计、编程、金融交易

等工作场景。

- 全面兼容（具备完整的浏览器兼容能力，满足网页对内核、插件、 C/S 应用的兼容要求）

1. 内核兼容

① 支持 Blink 和 IE 双内核；

② IE 内核支持多种模式切换：浏览器模式、文档渲染模式、 JS 引擎；

③ 基于规则库和网页特征自动切换。

2. 插件兼容

① 支持 NPAPI，PPAPI，ActiveX 插件；

② 支持网银，流版签等场景。

3. C/S 应用兼容

① 支持网页通过外部协议调起第三方应用；

② 支持下载并打开第三方应用；

③ 支持网页插件调起第三方应用。

- 极佳体验（云隔离平台带来沉浸式的体验，远程效果和本地使用保持完全一致）

1. 沉浸体验

① B/S 应用采用标签级融合，体验如同本地浏览；

② C/S 应用采用窗口级融合，体验如同本地应用。

2. 操作流畅

① 操作透传：输入法，快捷键，鼠标手势等；

② 流畅交互：快速响应，操作无延迟。

3. 高清显示

① 高清显示：自适应终端分辨率，支持 4K 高清显示；

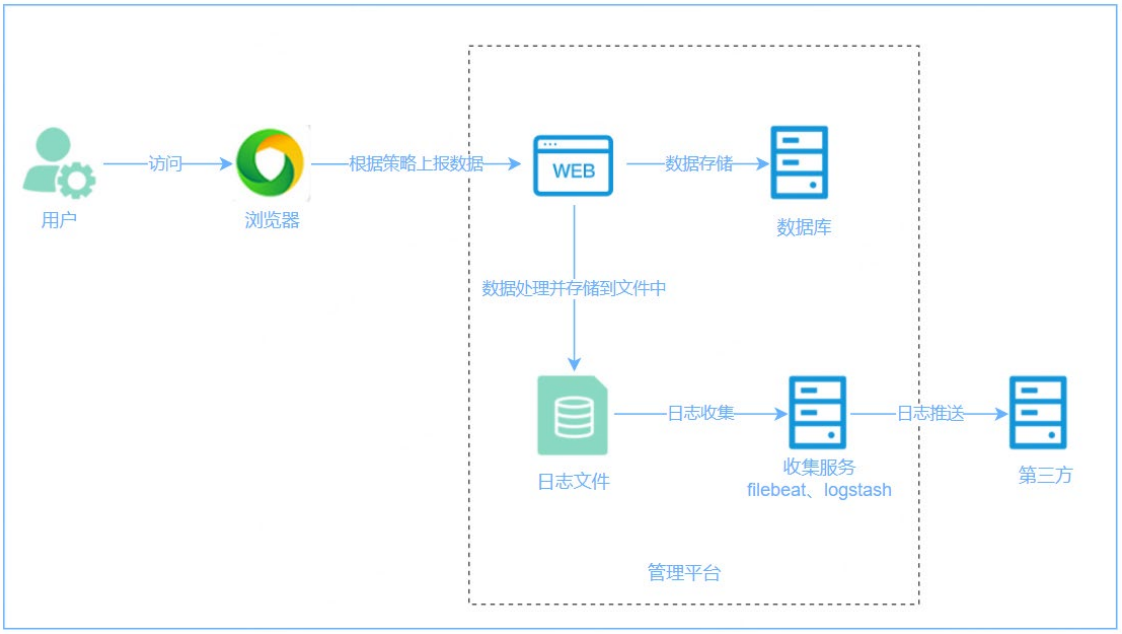
② 适应带宽：SNRS 技术自适应网络带宽，智能切换传输协议。

注：详细技术与功能介绍，请联系 360 安全浏览器团队获取《360 云隔离平台产品白皮书》

3.3.7. 日志审计管理

随着网络设备的逐步增多以及内外部的合规和建设要求，企业日志审计能力建设成为必须。运维人员需要付出大量的时间与精力投入到日志采集与分析中，如果没有日志审计功能

的辅助，将无法有效管理，多种设备之间也无法形成联系，容易形成信息孤岛。360 安全浏览器通过日志审计管理，可以将所有设备日志都收集到平台及进行统一管理、统一分析，不仅可以随时了解到业务系统的运行情况和及时发现系统中的异常事件，还可以通过事后的分析高效地进行针对性的安全审计，可以帮助管理员快速定位到安全问题。



用户在使用浏览器过程中，浏览器客户端会根据管理员在管理后台配置的策略，记录并生成相应的操作流水日志（如登录日志、访问日志、截图日志、安全防护日志、文件上传下载安全检查日志、文件关键字检测日志等），可根据需要开启对应的日志上报功能，开启后浏览器客户端将会通过加密通道向管理后台上传相关日志数据，第三方通过日志收集中间服务（filebeat 或 logstash 等服务）将日志传输到指定位置或存储介质中（如：kafka、elasticsearch、redis、mysql 等），管理员可查询或导出其管控范围内用户/设备的相关终端日志数据；管理后台也同时具备记录管理员的相关操作，形成管理员日志；管理员也可以管理日志的配置，如登录日志、截图日志、访问日志、管理员日志等数据的存储时长配置等。360 安全浏览器日志审计管理主要包括以下审计功能：

- 登录日志审计：在浏览器客户端使用账号登录浏览器后，客户端上报用户登录日志，日志数据包括但不限于用户名、登录 IP 地址、登录设备名称、登录时间、登录结果、客户端版本等。
- 访问日志审计：如需要针对特定应用进行访问日志采集，在策略管理开启应用访问采集策略，可针对指定应用进行访问数据采集，日志数据包括但不限于访问目的 URL、来源页面、来源链接、访问 IP、用户名、访问时间等。

- 截图日志审计：如需要针对特定应用进行自带截图日志采集，在策略管理中开启截图保护策略并允许自带工具截图，客户端通过自带截图工具截图后，可以将截图日志上报到管理后台。日志数据包括但不限于用户名、设备 IP 地址、设备名称、截图时间、文件名、客户端版本等。
- 安全防护日志审计:如需要采集用户在执行上传下载文件动作时的安全检查相关日志，在策略管理中开启文件安全检测策略，浏览器将禁止用户下载或上传特定等级的文件，以保护企业资产安全并记录日志。日志数据包括但不限于用户名、风险类型、设备 IP 地址、设备名称、防护结果、上报时间、文件详情、客户端版本等。
- 管理员日志审计：上级管理员可以查询其管控范围内的管理员操作记录日志数据。日志数据包括但不限于：用户、设备 IP 地址、管理员角色、操作模块、操作项、操作时间等。
- 文件关键字检测日志审计：在文件上传时针对文件内容进行关键字检测，并可以实时返回检测的结果，记录检测日志。日志数据包括但不限于：用户、应用名称、扫描时间、文件路径、文件名称、设备 IP 地址、文件上传结果、扫描结果、触犯的关键字等。

3.3.8. 策略配置参数的沙箱机制

用户在使用 IE 浏览器时一定遇到过这样的场景：自己好不容易配置好的可以正常访问某个业务系统的浏览器设置，在访问业务系统的时候又不正常了，去查看相关配置项时发现配置不知道什么时候又被改掉了，非常令人头痛，这种情况一般是由于某些第三方软件处于对自己有利的目的（一般是商业目的）去修改浏览器的某些参数项，由于 IE 浏览器的所有配置项都是在系统注册表中，而那些第三方软件在安装时都会有提权操作要求，所以修改相关的注册表项也都是比较顺手的事情。

在 360 安全浏览器中的配置参数是通过配置沙箱的概念来进行保存和读取的，它被保存在受保护的内存区域里，不会写入本地注册表，从而有效防止第三方软件的篡改和污染。

3.4. 标准构建

3.4.1. 浏览器标准

在工作场景的跨平台统一浏览器标准，是企业生产运营至关重要的布局建设，确定的浏览器品牌型号、内核版本特性、功能性能、平台适配能力，都可以大大降低业务开发、安全建设等环节时可能存在的隐患和不确定性。

3.4.2. 业务开发标准

360 安全浏览器提供整套 Web 开发标准规范，支持企业在信息化建设过程中，依托 360 安全浏览器作为基座标准，进行业务系统的适配开发。

注：如有需求，请联系 360 安全浏览器团队获取《业务开发指南》

3.4.3. 信创 B/S 迁移标准

360 安全浏览器提供整套业务系统在信创领域迁移时的全方位服务，包括但不限于成熟稳定的迁移兼容性检测工具、迁移兼容性修复工具、迁移工程管理工具、迁移专家指导服务。

注：如有需求，请联系 360 安全浏览器团队获取《产品使用及开发指南》

3.4.4. 信创 C/S 迁移框架（易创）

360 安全浏览器的全面异构适配能力，支持企业在 C/S 信创迁移过程中，几乎 0 成本的完成 Electron 框架、CEF 框架在信创平台的迁移。

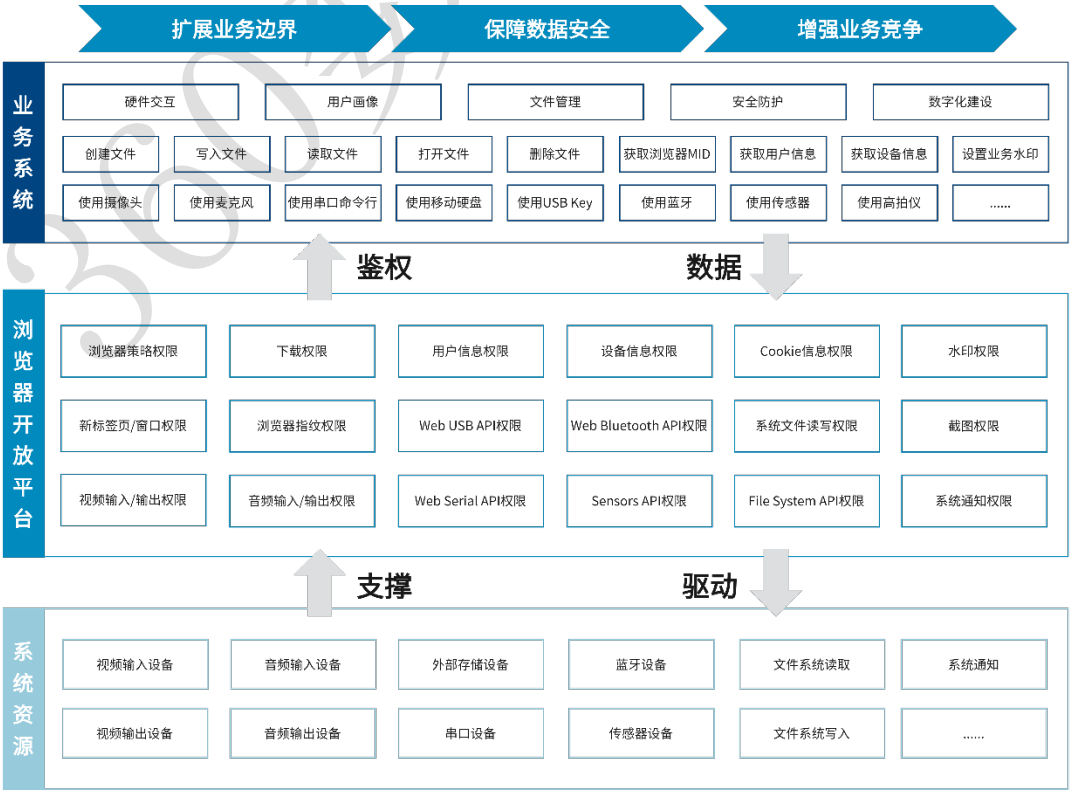
注：如有需求，请联系 360 安全浏览器团队获取相关支持。或直接访问官网：https://yichuang.360.net/

3.4.5. 应用级 Web 载体

360 安全浏览器能够提供全套浏览器开放接口，包括常规接口和 360 独有接口，通过安全接口底层设计，全面支撑各类 Web 应用以 360 安全浏览器作为载体，完成兼容适配、安全加固加强、业务开发效率提升等诉求。

3.5. 协作联动

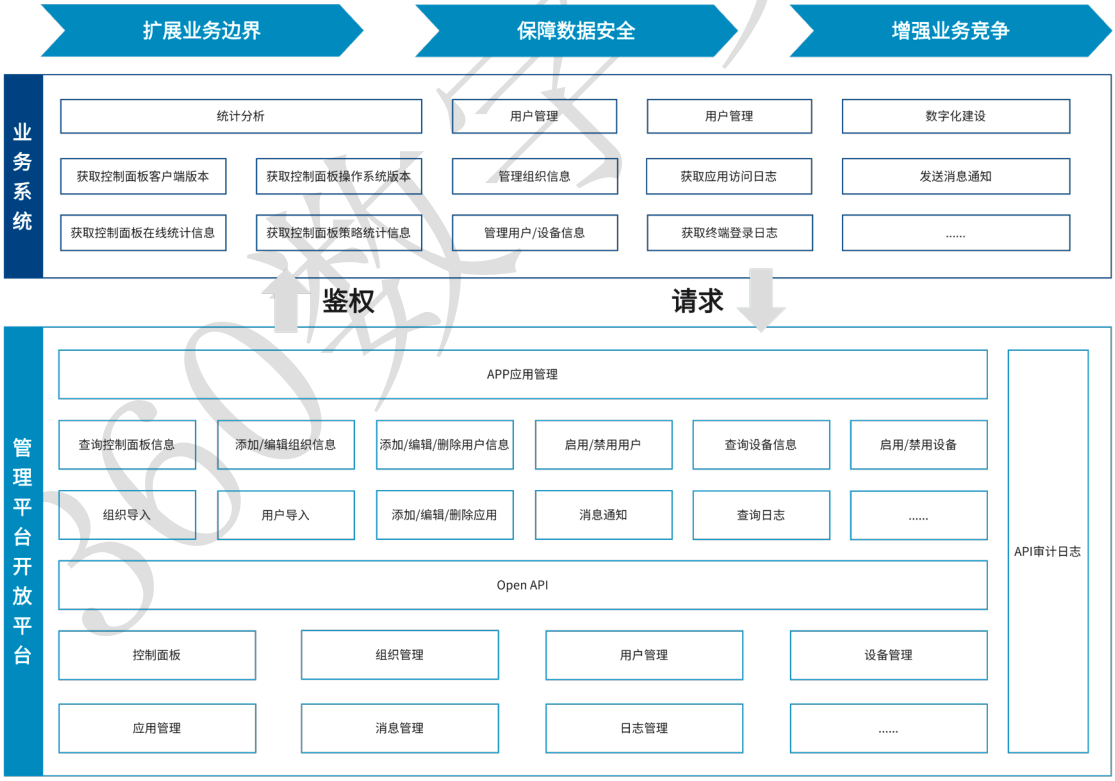
3.5.1. 客户端开放 JS-API 接口



B/S 应用因其在使用过程中，对于客户端底层的屏蔽能力，使得 B/S 架构应用在推广过程中免除了很多的多平台适配、升级问题。但同样由于 B/S 应用这种屏蔽能力，隔绝了应用对于客户机本身的访问能力。例如应用无法获取设备本身的 IP 地址、设备识别码等，应用也无法对客户机进行操作。这些操作本身其实违背了 Web 应用的安全规范，但是在安全性相对可控的企业环境中，进行这些操作有存在的一定合理性。360 企业浏安全览器针这些在应用过程中可能用到的 API 功能，在页面 JavaScript 中增加了 API 能力，使得页面在进行认证后可以与浏览器进行交互，进而使用浏览器客户端运行环境的一些能力，比如获取客户端本地信息，与浏览器功能进行交互等。为企业应用功能拓展新的边界。

目前可以获取到的开放 API 接口包括：页面水印、网页通知、截图保护、访问 Cookies、用户信息、设备信息等。

3.5.2. 管理平台开放 API 接口



企业在信息化建设过程中，对业务办公安全愈加重视，管控颗粒度也愈加细致。360 安全浏览器具备可以管控所有办公浏览器的能力外，也同时可以根据企业业务场景，分别对内外部数据进行安全接入和输出，比如企业自建大数据平台的数据可视化场景，其他业务系统的消息通知与管理平台和客户端的联动推送。

目前支持通过管理平台开放 API 接口，可以获取到的能力包括：消息通知、组织管理、用户管理、用户信息、设备信息、日志查询、策略下发、认证下发等。

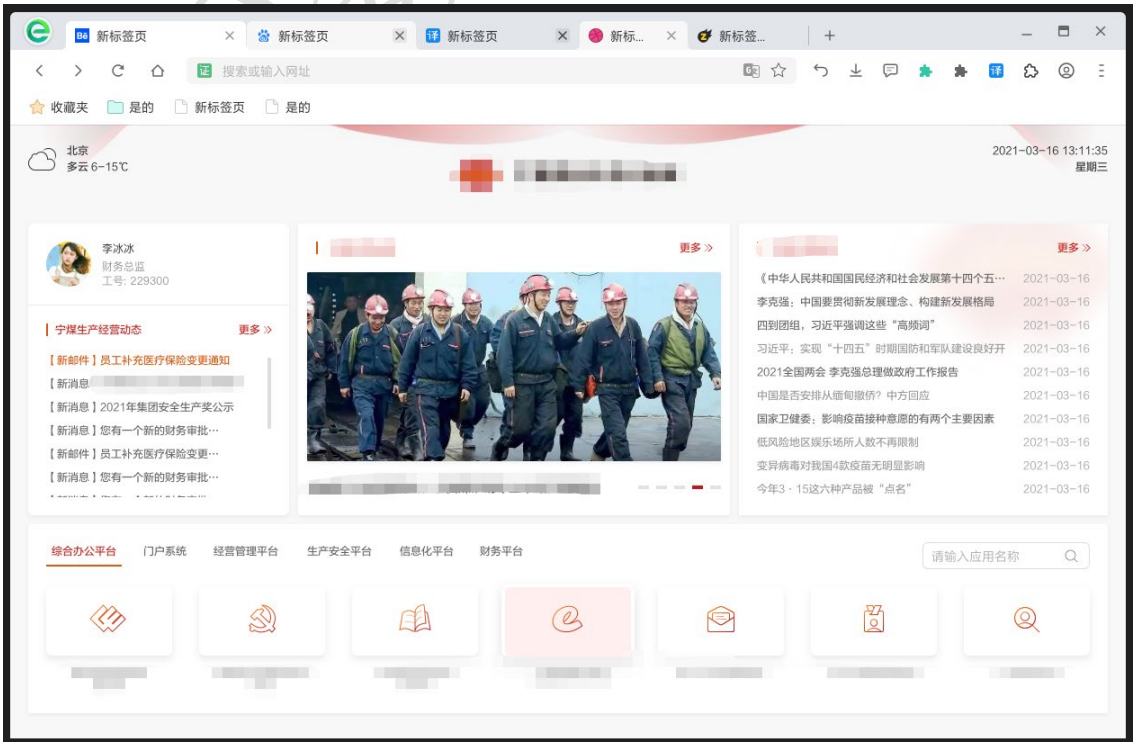
3.5.3.业务深度融合

3.5.3.1.消息通知融合

可以针对全体员工及不同的部门下发统一的消息，设置消息的消息体图片、标题、摘要、logo、消息下发的 URL 及时间段；管理员可以看到消息的送达数及点击数及下发的状态，对消息进行增、删、改、查等操作。

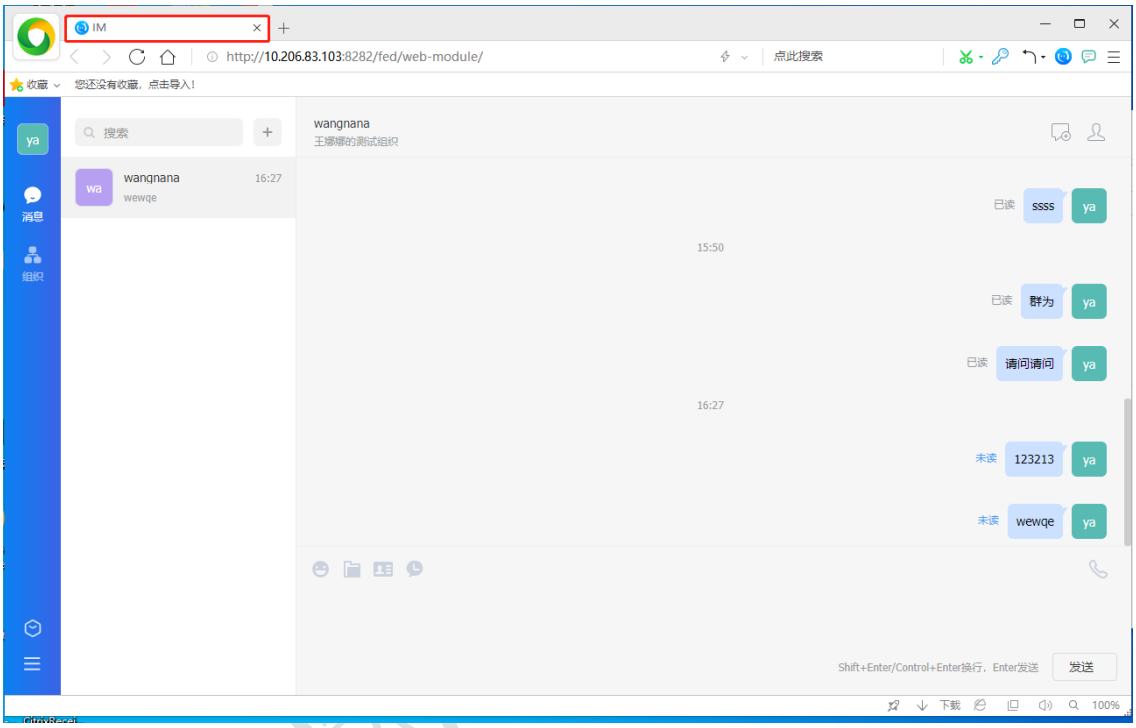

全选
标记为已读
删除
2020/07/30
入职纪念
亲爱的张三：
值得纪念的日子，360因为有了你而更加美好，感谢你对公司做出的贡献，在此祝你生日快乐!事事顺心!
制作专属贺卡
YouTube
2019/12/08

3.5.3.2.门户导航融合


新标签页
收藏夹
北京
多云 6-15℃
2021-03-16 13:11:35
星期三
综合办公平台
门户系统
经营管理平台
生产安全平台
信息化平台
财务平台

360 安全浏览器的门户导航，将提供诸多开放接口，提升诸多与终端设备、业务应用系统等维度进行融合对接的方式。

3.5.3.3.即时通讯融合



360 安全浏览器支持与企业内部即时通讯产品的深度融合，通过浏览器客户端可以快速对接 WebIM 植入。

3.5.4.浏览器数据可视化

- 集中监控引擎

企业业务系统由 C/S 架构转向 B/S 架构已经成为事实，浏览器客户端成为企业员工日常 PC 办公的重要入口，那么浏览器用户在办公场景下的行为操作，将会成为企业经营过程中重要的数据源。360 安全浏览器可根据运维管理员的授权下对浏览器客户端进行集中监控采集，包括但不限于终端层、应用层、用户层、安全层的数据监控采集，所有采集后的数据都存储于本地私有化环境中。

同时 360 安全浏览器的集中监控引擎还支持提**供数据公共资源池**的能力，可以提供相关监控数据输出的能力，推送相关数据到企业自建的大数据平台进行分析和消费。

- 数据分析引擎

集中监控引擎每日数以亿级的数据量将会通过数据分析引擎的配置进行过滤筛选、清洗处理、分析建模后，输出相应结果以供其他业务使用。

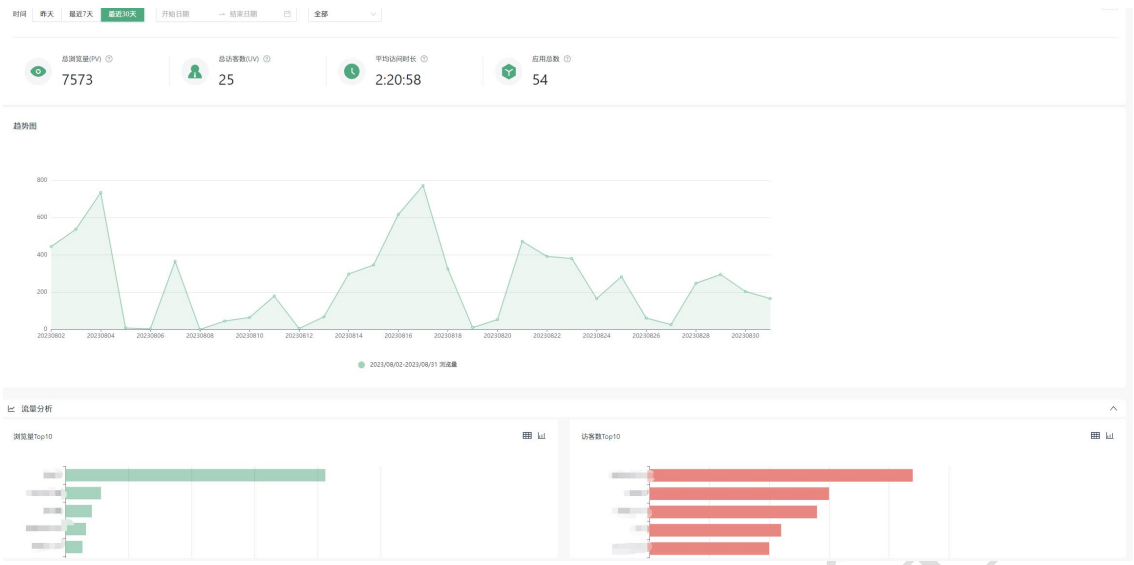
- 场景预警引擎

场景预警引擎与集中监控引擎和数据分析引擎组成引擎三角，根据算法对历史数据进行深度挖掘，形成浏览器客户端的各类场景模型运行基线，再结合集中监控引擎的实时数据比对后，作出相应预警或处理。

- 态势可视化引擎

态势可视化引擎可根据配置，对接集中监控引擎、数据分析引擎、场景预警引擎的业务结果展示或数据展示，通过拖拽即可进行模板引入和数据对接。

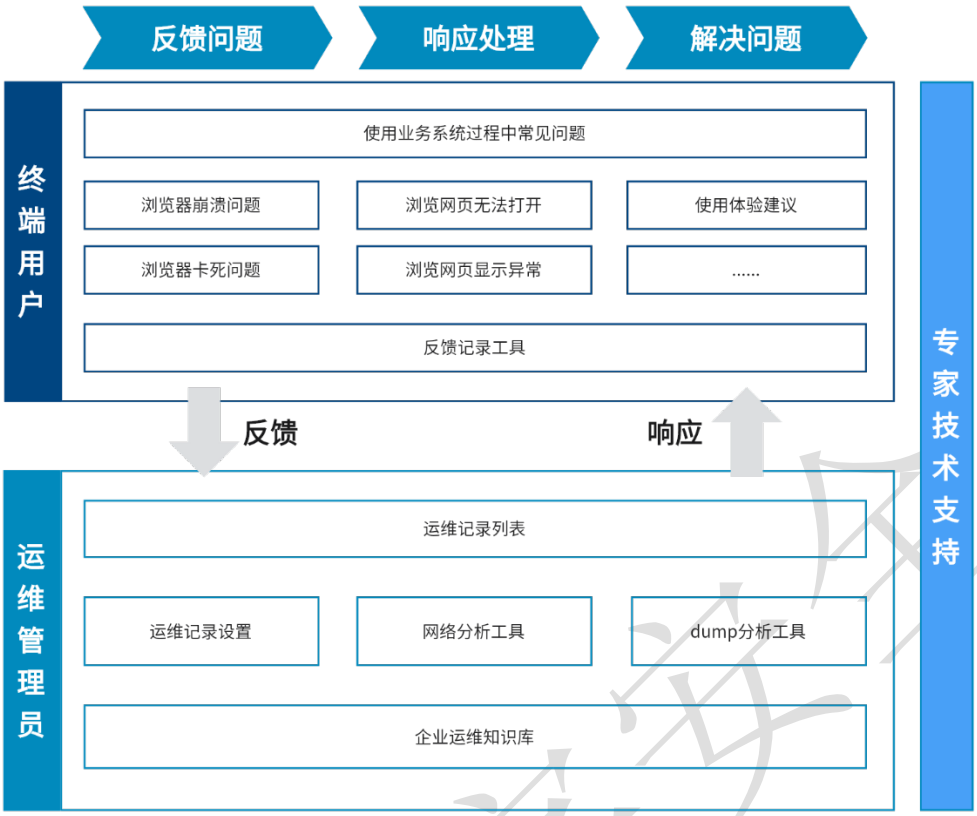
相关数据演示案例如下：



3.5.5. 运维反馈收集

360 安全浏览器支持全平台浏览器客户端的运维反馈收集功能，包括浏览器客户端运行状态收集、业务系统运行状态收集、用户体验反馈收集等功能。

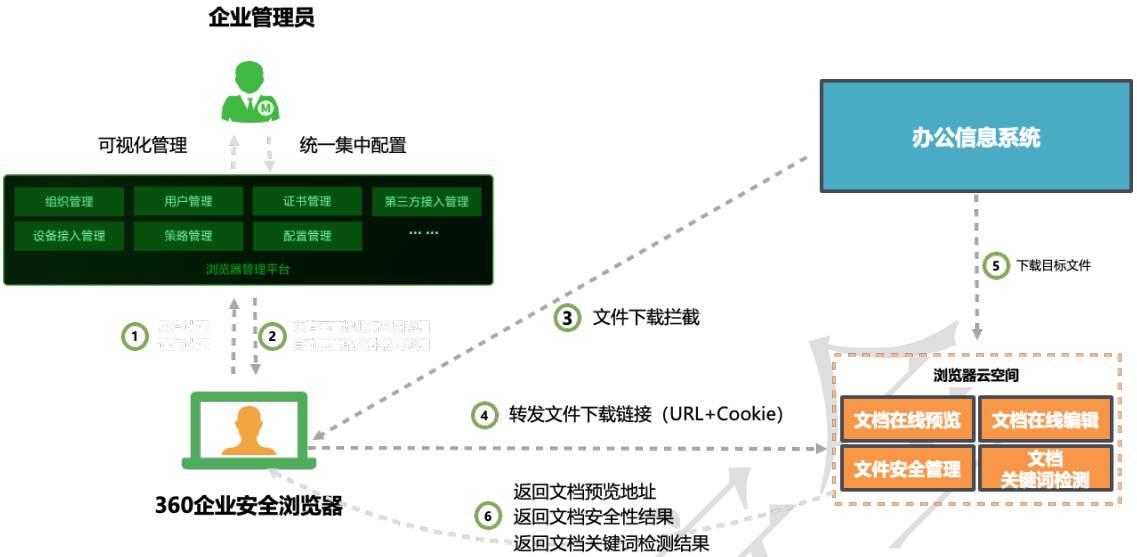
在企业推广业务系统的过程中，发生浏览器故障或业务系统问题时，存在解决效率低下、终端用户无法联系到运维管理员、管理员运维工作无记录等问题，企业级浏览器的运维管理模块可以一站式解决这些问题。



企业级浏览器运维管理模块，已经形成了从反馈问题，响应问题，最后解决问题的完整闭关模型。终端用户在使用业务系统过程中遇到的诸如浏览器崩溃、卡死、无法打开、显示异常等问题，可以通过反馈记录工具，将问题记录报告至管理平台，运维管理员可以在管理平台的运维记录列表中响应处理相关问题，并可将处理建议或动作传递至终端用户。

运维管理模块，为企业业务推广、日常运维工作，提供了统一输入平台，建立了 B/S 架构业务标准化的问题处理流程，帮助企业建立完善的内部知识库体系，提升终端用户使用体验，提高业务处理效率。

3.5.6. 浏览器云空间



通过浏览器拦截业务系统上传、下载操作并转发给浏览器云空间，可以在业务系统不做改造的前提下实现文档在线预览的目的

浏览器支持内置云空间，将企业用户使用浏览器过程中实现，文档在线预览/编辑、文件关键词检测、文件安全性检测、文件安全管理等功能。管理员可根据企业内审和安全要求，对组织部门、文件类型进行如下配置：

- 从业务系统下载的文件直接存储到云空间（包括云隔离访问过程）
- 从业务系统上传的文件从云空间进行选择
- 从业务系统下载的文件只能在线预览和编辑
- 从业务系统上传、下载的文件，对其进行安全性检测
- 从业务系统上传、下载的文件，对其进行文件关键词检测

4. 产品特点及优势

4.1. 产品优势

4.1.1. 市场检验时间长、稳定性高、客户认可度高

360 安全浏览器经过 10 多年的发展，活跃用户达到 4.03 亿，市场渗透率 81%，每天恶意网址扫描达到 200 亿次，拦截恶意网址 2000 万次，是国内市场占有率第一的浏览器产品；360 安全浏览器是在继承了安全浏览器产品的安全性、高性能、健壮性的基础上针对办公场景所

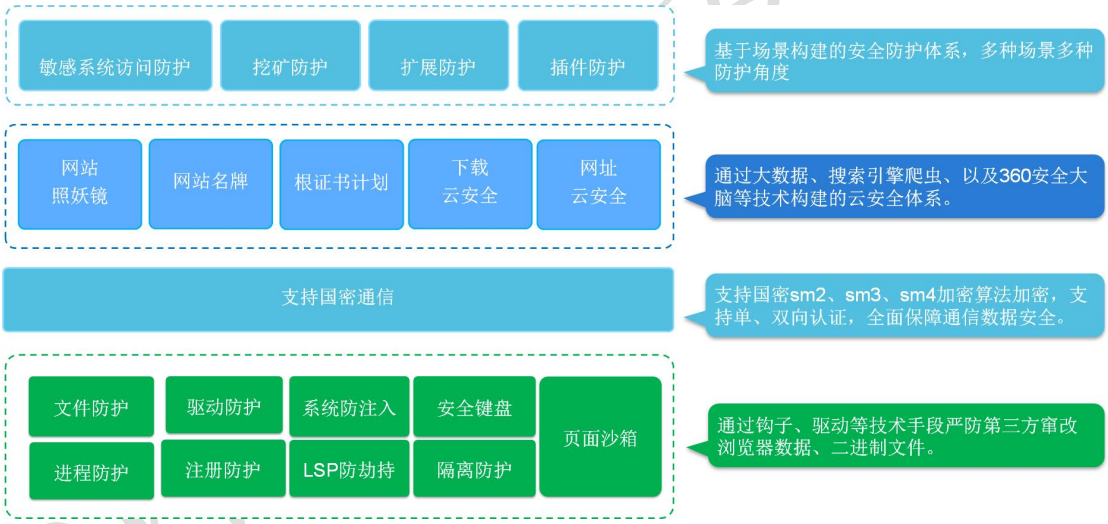
开发的专用工作平台。

4.1.2. 自主可控度高，问题排查能力强

360 安全浏览器拥有 10 多年的研发经验，基于最新版本的 Blink 内核进行开发。360 对浏览器内核具有完全的自主掌控能力，能够有效解决应用过程中发现的各种技术问题，并且 360 安全团队具有漏洞发掘能力和及时的漏洞修复能力，为浏览器安全上网过程提供多角度安全防护措施。

4.1.3. 16 层安全防护，全方位立体保护 Web 应用办公安全

360 安全浏览器能根据应用的特点，分别提供系统安全、云服务安全、内核安全、进程隔离安全、第三方服务安全等 5 个方面共计 16 层安全防护能力。



- 浏览器系统安全：采用多进程架构，网页、代码、插件、扩展、GPU 等进程相互隔离。
- 浏览器进程安全：利用已有的沙箱机制，对沙箱里的应用进行控制，用户无论的输入是什么，沙箱都能最终确决定能做什么或不能做什么。
- 浏览器内核安全：内核脚本引擎应用能将不同的页面和扩展运行在不同的隔离域，从而保证它们不会相互访问和污染，不同隔离域的脚本不能互相访问、非同源的脚本上下文之间不能互相访问，能够自动识别 XSS 攻击代码，并对该请求进行屏蔽。
- 数据安全：包括访问历史、收藏、缓存、Cookie 等和用户浏览状态历史相关的数据。为了防止用户数据被其他应用篡改甚至拷贝，浏览器针对一些用户的隐私数据进行

保护，比如 Cookie 信息、历史记录、保存到本地的表单密码、用户收藏的网址等等，这些数据在本地采用对称加密算法，这些算法用到的密钥一般都采用特殊算法保存在本机，可以实现即使隐私数据被盗取的情况下，也是无法解密并读取其内容的。

4.1.4. 全面支持国密证书、双向认证功能

360 安全浏览器在信创平台上实现了基于商用密码算法对用户证书及 USBKey 设备的操作、使用用户证书实现身份认证、完成与服务端的 SSL 安全连接、对客户端和服务端的数据传输进行加解密等业务流程，且 SSL 通道支持单向、双向认证，其中单、双向认证采用了双证书机制，并全部使用国家密码主管部门认可的算法，一方面符合了国家有关密码使用的相关要求，也能有效保证数据安全。

4.1.5. 浏览器功能丰富，用户个性化定制体验选择多样

360 安全浏览器客户端界面风格、管理平台界面风格、功能配置设置等，均支持快速定制与交付。

4.2. 价值定位

- 工作统一入口

以 360 安全浏览器为载体枢纽，作为工作统一入口衔接企业内外部员工、业务应用和终端。

- 工作安全防线

360 安全浏览器内包含近百项安全功能，可补全企业工作场景中的安全盲区和安全中转，将安全防线前移到用户操作浏览器前中后期，并支持与其他企业内部已有的三方安全产品联动，提供一套以 360 安全浏览器为载体的数据安全、业务安全、身份安全解决方案。

- 业务应用载体

360 安全浏览器具备强大的可扩展、可联动的基础能力，成为业务应用的最佳载体，降低业务应用在实现过程中的技术门槛和路径。

- 业务应用操作系统

360 安全浏览器以自身多种标准与规范，升级为应用级操作系统，保障业务应用的标准化输入与输出。

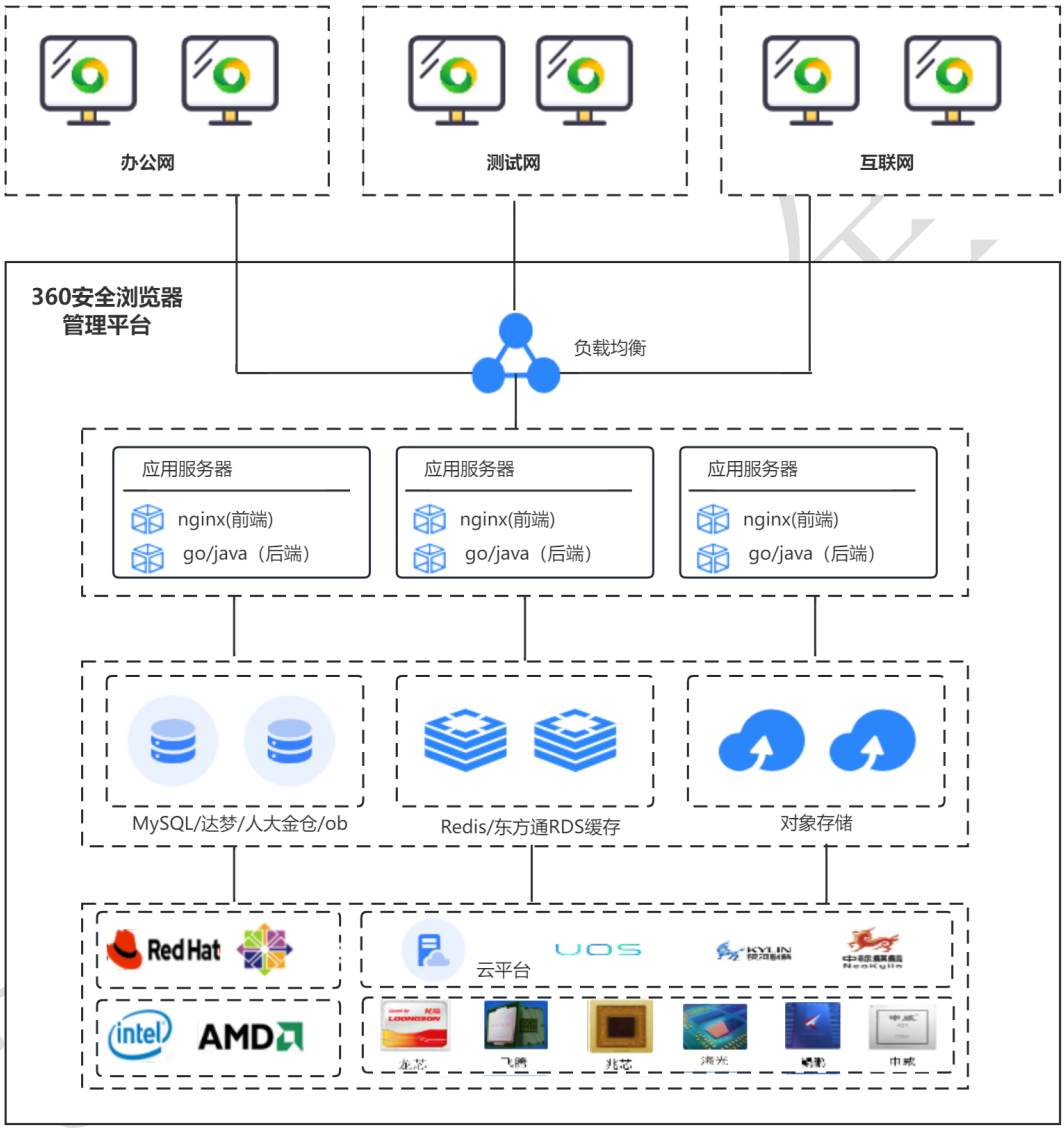
- 生产运营平台

360 安全浏览器具备最贴近用户、终端、业务的特性，能够根据企业要求细颗粒度的承载和补全生产运营过程中的关键数据输出与关键事件输入。

- 降本增效生产力

360 安全浏览器拥有一套平台管理统筹全局业务融合的价值，是效率协作、安全协作的关键生产力。秉承让专业的人做专业的事，通过集中化配置管理、双核自动切换、浏览器渲染行为模拟、弹出窗口管理、IE 配置同步、控件管理等方式一站式解决企业中兼容性要求不一的业务系统带来的页面访问麻烦，从而大大减少普通用户在使用过程中的复杂程度，提高整体企业效率，降低企业资源的损耗。

5. 典型部署



360 安全浏览器管理平台支持单机、分布式集群、云平台、信创环境部署，满足高可用、高性能部署要求，支持达梦、人大金仓、优炫、oceanbase 等国产数据库、支持东方通 RDS、东方通 THS、东方通 Tongweb 等中间件，全面适配国产芯片和操作系统。

6. 公司介绍

360 集团创立于 2005 年，是中国最大、全球领先的网络安全公司和最有影响力的互联网公司之一，也是人工智能、大数据领军企业。2015 年，360 从美国退市回归 A 股。2018 年 2 月，360 成功在国内 A 股上市，成为纯内资网络安全企业。目前，360 已成为国家网络安全保障的核心力量，在十九大、两会、九三阅兵、“一带一路”峰会、上合组织峰会、金砖会议、APEC 等重大活动，以及国家安全和国防安全相关工作中发挥了重要作用。

2017 年，360 提出“大安全”战略，把网络空间安全与国家安全、国防安全、城市安全、基础设施安全以及人身安全等进行统筹谋划和整体布局。2018 年，360 提出安全大脑是应对“大安全”时代新威胁和大挑战的技术方向和思路，要共建国家安全大脑、城市安全大脑和家庭安全大脑，捍卫国家网络安全，维护城市和社会安全，为老百姓提供安全感。2019 年，360 全面进军政企市场，落地“大安全”战略，打造安全产业生态，为国家安全保驾护航。

7. 引用资料：

1. 《DBIR 2023 Data Breach Investigations Report》：
https://www.verizon.com/business/resources/T7b/reports/2023-data-breach-investigations-report-dbir.pdf

2. 《威胁猎人-2022 年数据资产泄露分析报告》：
https://www.threathunter.cn/reportDetail/eaeff5f5fb5e75cfec880a496fe54940