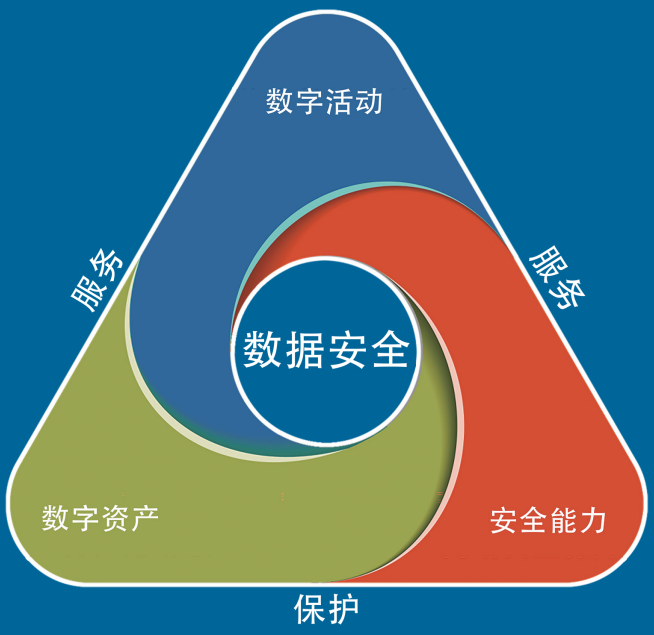
数世咨询
Digital World Consulting

企业浏览器能力指南

数世咨询
Digital World Consulting

企业浏览器能力指南



数字安全的三个元素分别为，安全能力、数字资产和数字活动。数字资产是安全能力的保护对象，数字活动是安全能力以及数字资产的服务对象，而数据安全则是三元论的核心目标。对于这四者关系的深度理解和相关技能掌握是做好数字安全工作的关键。

数字安全能力模型研究的基础，来自于数世咨询 2020 年首次提出的“网络安全三元论”。三元分别为，网络攻防、信息技术和业务场景。

随着数据成为第五大生产要素为典型标志的数字时代来临，“网络安全三元论”在 2022 年进行了更新迭代升级为“以安全能力、数字资产和数字活动为三元素，以数据安全为核心目标，即三元一核”的“数字安全三元论”，以适应我国数字中国建设的进程。

数世咨询作为国内独立的第三方调研咨询机构，为监管机构、地方政府、投资机构 . 网安企业等合伙伙伴提供网络安全产业现状调研，细分技术领域调研、投融资对接、技术尽职调查、市场品牌活动等调研咨询服务。

报告编委

主笔分析师 **闫志坤**
分析团队： **数世智库** 数字安全能力研究院

目 录

目 录

前　言

随着数字化进程不断推进，安全访问越来越受关注，几乎所有的应用访问都基于浏览器，浏览器成为安全访问的核心切入点。浏览器作为一种开放式软件平台，不仅用来访问私有应用，还可以访问互联网上的海量资源，因此，浏览器逐渐成为所有业务访问的统一入口。

无论是在家办公还是远程办公，员工在工作或个人目的访问互联网时都会高频使用浏览器，然而，需要注意的是，它并不是为安全而设计的。目前，浏览器已成为黑客渗透攻击的重要目标，攻击手段包括恶意软件和病毒、钓鱼攻击、跨站点脚本（XSS）攻击、拦截与篡改通信、浏览器插件漏洞、零日漏洞等。

数世咨询认为，面对业务需求和安全需求，组织内使用的传统浏览器将要转向企业浏览器，企业浏览器成为业务访问的统一入口。

随着信创工作不断推进，从政府部委到央国企，很多办公业务系统均迁移到信创平台。由于企业浏览器可以兼容各种信创 CPU 和操作系统，以及相应的业务应用（包括信创应用），同时支持国密算法和国密证书，这也成为了政企组织率先采购企业浏览器的主要驱动因素之一。

此外，**企业浏览器不仅自带安全功能，而且还可以集成其他安全模块，**能够有效防止用户遭受网络攻击、恶意软件入侵、网络钓鱼并提供可靠的数据加密和隐私保护功能，以保障用户数据的安全性和完整性，这种特性使得用户可以在浏览器中完成多种任务，无需安装多个应用程序，从而大大减少了用户因工作需要下载各种软件的风险，也没有设备要求的限制，实现全场景的统一访问。同时，企业浏览器还具备统一管理功能，可以进行兼容配置管理、拓展管理、插件管理、策略管理、Web 访问控制、操作行为管控、集中配置下发以及浏览器更新补丁等。

鉴于上述背景，数世咨询撰写本报告。

勘误及交流请联系本报告主笔分析师闫志坤：yanzhikun@dwcon.cn。

关键发现

1、目前几乎所有的应用访问都基于浏览器，浏览器成为统一访问的核心切入点；

2、传统浏览器存在巨大安全风险，已成为黑客渗透攻击的重要目标，如何提高浏览器的安全性，成为组织亟需解决的问题；

3、央国企信创的全面铺开，在硬件、操作系统、业务信创改造时，浏览器也需要升级以实现兼容适配，保障业务正常使用；

4、面对业务需求和安全需求，组织内使用的传统浏览器将要转向企业浏览器，企业浏览器将成为业务访问的统一入口；

5、对于用户而言，企业浏览器自带安全属性，并可以通过模块化增加防病毒、终端环境感知、ZTNA 的能力，实现了多种客户端的统一化，大大减少单一安全应用程序的安装部署，减少 PC 性能损耗；

6、为了应对安全访问的安全挑战，一种策略是 SSE（安全边缘服务）将访问统一接入到边缘云；另外一种策略是将访问统一接入到企业浏览器，企业浏览器具有集成方便、成本低、用户实际体验效果好等特点。

1、企业浏览器概念描述

本报告中，数世咨询对企业浏览器（Enterprise Browser ）描述如下：

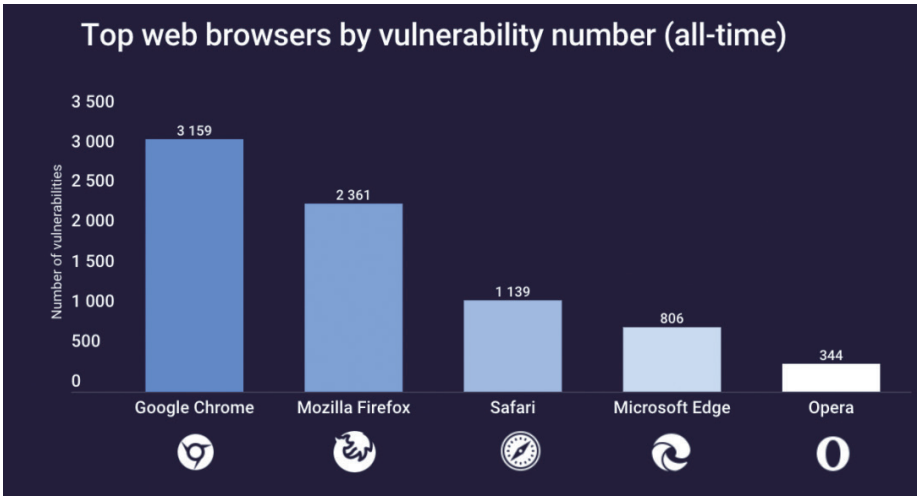
是针对办公环境（如企业、政府、教育机构等）需求设计的新型浏览器。与传统浏览器相比，企业浏览器具备更强的安全性、跨平台兼容适配、统一管理、高效工作、合规性等特色功能。

分类 / 功能	传统浏览器	企业浏览器
用户画像	个人用户	政企用户
安全性	一般	更强
统一管理	无	支持
浏览器插件/拓展管控	无	支持
产品架构	客户端	客户端+管理平台
应用兼容性	部分业务应用	所有业务应用
部署方式	本地部署	本地部署和分布式部署
企业定制	无	支持
服务支持	无	支持
商业模式	免费	收费

企业浏览器出现的背景：

1.1 传统浏览器成为黑客攻击的重要目标

根据浏览器安全平台提供商 LayerX 发布《2023 年浏览器安全调查》报告，浏览器账户攻击是重灾区，48% 的受访者将凭证网络钓鱼视为风险最高的浏览器威胁，其次是恶意浏览器扩展（37%）、恶意软件下载（9%），以及浏览器漏洞（6%）。另外，全球 60% 的企业遭受过恶意软件攻击。



根据 VPN 服务提供商 Atlas VPN 2022 年分析报告，谷歌 Chrome 浏览器在其整个生命周期中总共经历了 3159 个漏洞，Mozilla Firefox，自发布以来总共发现了 2361 个漏洞；苹果的 Safari 总共有 1139 个安全漏洞；Microsoft Edge 自 2015 年推出以来发现了 806 个漏洞；Opera 自发布以来一共发现了 344 个漏洞。

1.2 业务需求与安全合规的双重驱动

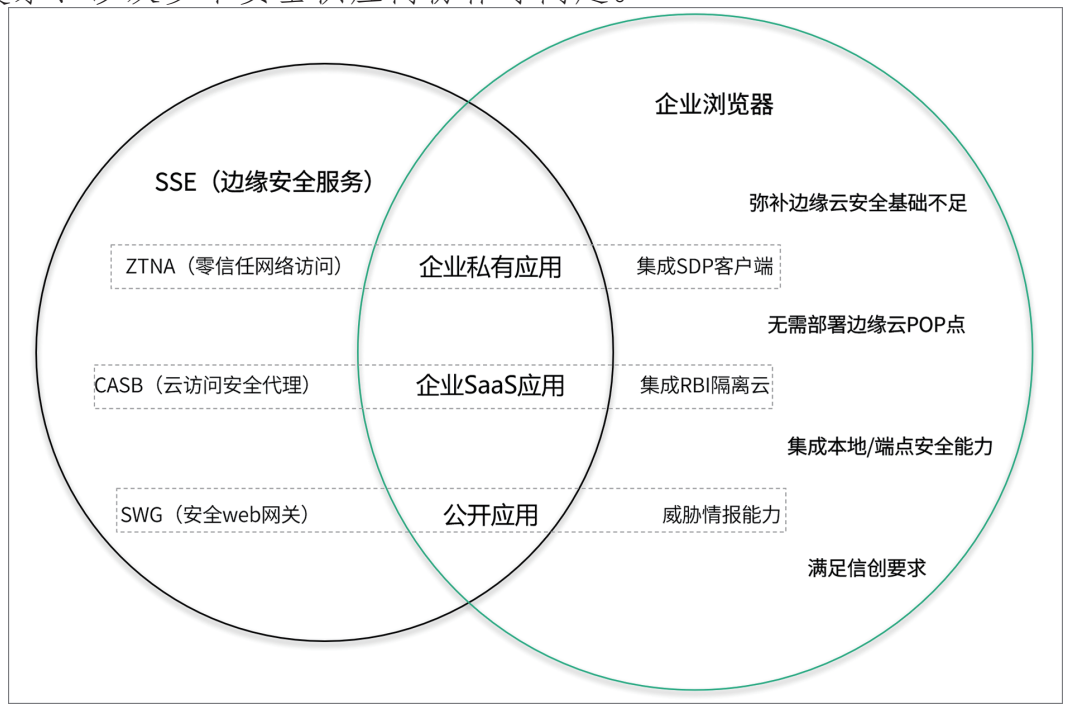
随着央国企信创的全面铺开，在硬件和操作系统升级时，也需要对 B/S 业务系统、业务应用 APP 或应用程序等进行信创国产化改造，企业浏览器要做好跨平台兼容适配，保障业务正常使用，成为所有业务访问的统一入口，同时满足国密通信协议等安全要求，有效保护用户的数据通信安全。

1.3 组织有效提高生产力的关键抓手

在办公场景中，浏览器是一个高频刚需的办公软件。根据 Forrester Consulting 调研数据，员工有 75% 的日常工作是在浏览器上完成的，而在组织中，使用浏览器工作的人高达 96%，因此，**浏览器成为业务访问的统一入口，选择一个符合要求的浏览器对于提升组织的生产力至关重要。**企业浏览器本身具备统一应用入口、应用兼容适配、风险网址拦截、恶意代码检测、可信应用授权管理等基本功能。因此，企业浏览器凭借应用导航、兼容适配、用户实际体验效果好等特点，可以有效提升员工生产力。

1.4 企业浏览器成为安全访问的新赛道

面对企业私有应用访问、企业 SaaS 应用访问、互联网公开应用访问的安全防护难题，业界提出很多创新技术，例如 SSE（安全边缘服务），主要由 ZTNA（零信任网络访问）、CASB（云访问安全代理）、SWG（安全 web 网关）三大部分组成，而国内边缘云安全基础不足，落地 SSE 需要通过云地协同方式，不仅需要在边缘处部署 POP 点，还需要本地部署安全防御能力，因此存在整体架构复杂、涉及多个安全供应商协作等问题。



SSE 与企业浏览器功能对比

企业浏览器通过集成安全模块的方式亦可解决多场景的安全访问难题，首先针对企业私有应用访问，在企业浏览器管理平台上集成 SDP 客户端就可以构建零信任网络实现安全访问，与终端环境感知能力协同，以增强身份认证和访问行为管控能力；其次对企业 SaaS 应用安全访问，通过 DLP、应用审计及集成 RBI 远程浏览器隔离技术，实现安全隔离访问、恶意网址拦截、文档在线预览、操作行为审计等功能，而对于访问公开应用的安全防护，则是企业浏览器自身安全能力 + 威胁情报即可实现，例如风险网址拦截、URL 过滤、Web 访问控制、行为管控、高敏网站访问安全等功能。

相比 SSE（安全边缘服务），边缘云主要采用公有云形式，企业浏览器主要满足本地部署和私有云部署；国内边缘云安全基础不足，企业浏览器管理平台自带常用安全能力，无需部署其他安全设备，同时企业浏览器满足跨平台兼容的信创合规要求。企业浏览器在安全功能加持下形成客户端 - 控制中心 - 网关的安全访问架构，可以解决上述三大场景下的安全访问难题，成为了安全访问的新赛道。

2、用户需求与痛点

2.1 解决兼容适配

为了正常访问多个业务系统门户，员工在 PC 终端可能需要安装不同种类、不同版本的浏览器去适配应用系统。这样无疑造成本地资源浪费、导致工作效率低下。

因此通过统一的浏览器去适配和兼容不同厂商、不同版本的浏览器内核引擎，适配工作做到对用户完全透明，减轻用户的重复繁琐设置操作。

2.2 实现统一管理

组织中存在各类业务应用系统且用户繁多，当业务系统升级需要对终端浏览器安装新插件或更新版本时，每个终端都需要手工去执行操作，增加了业务人员工作负担，且有时候会误操作，导致升级失败或引入第三方不安全插件，造成部分紧急任务未及时处理，降低工作效率。

因此亟需统一管理功能，实现统一配置管理、双核自动切换、统一访问入口、弹出窗口管理、IE 配置同步、控件管理等方式，解决不同业务系统不同兼容要求带来的页面访问问题，从而大大降低普通用户在使用过程中的复杂程度，提高整体企业工作效率。

2.3 加强安全防护

浏览器在使用过程中，面临着外部访问时恶意网站攻击、下载文件是否安全、网站证书是否过期、仿冒、是否存在恶意进程；特别是涉密数据尤其是人员档案、财务明细等面临着下载、打印、复制、拍照、分享等的数据泄露风险

及用户本地数据（历史、收藏、缓存、Cookie）泄露风险等。

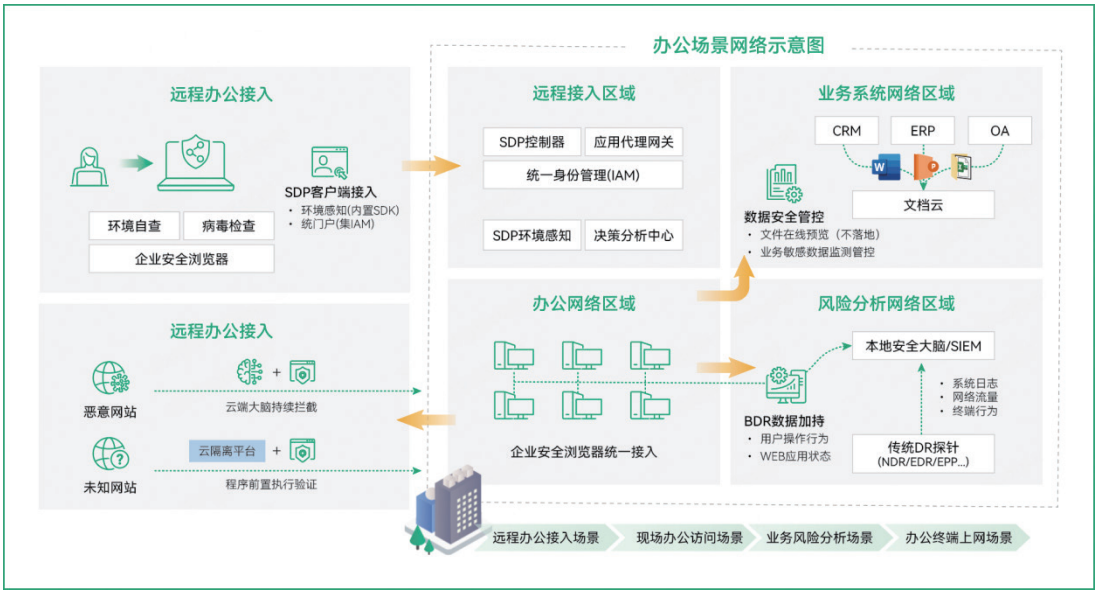
因此，加强浏览器安全事关重要，从各个维度完成数据安全防护。从启动浏览器开始工作，到业务访问结束退出浏览器，在接入管控、传输安全、数据防泄密、威胁发现等重要场景进行安全防护，同时提供完整的日志管理，大大保障了企业机密数据的完整性和安全性。

2.4 远程访问安全

远程办公越来越流行，组织在的 VPN 远程办公暴露了诸多问题，首先就是不稳定，使用 VPN 工具连接到公司内网时经常遇到连不上、频发掉线；其次是不安全，传输网络安全和用户授权、用户行为风险等，最后，易用性问题，很多 VPN 客户端上手难、不稳定，经常需要重新安装或重启电脑才能解决。

因此，在企业浏览器上集成基于零信任理念的 SDP 架构成为最佳方式之一，员工无需单独安装应用程序，集成身份认证，无感访问各个业务系统；IT 运维部门统一管理，进行细粒度的访问控制，持续验证用户身份是否可信，以确保在终端访问数据的应用安全可靠，达到安全、稳定、易用的真实需求。

3、技术框架与核心功能



企业浏览器技术框架

为了确保访问安全，企业浏览器采用了客户端 + 管理平台设计。首先，针对 Windows 操作系统，安装双内核客户端，即 Blink 内核和 IE 内核。而对于信创操作系统和 Mac 操作系统，则仅安装 Blink 内核客户端。这些客户端都由企业浏览器管理平台进行统一管理，可以下发各种策略，这些策略包括但不限于行为管控、应用导航、准入策略、私有拓展管控和内核切换等。

此外，企业浏览器管理平台还具备信息下发功能，可以发送消息通知和第三方通知，还能收集用户的反馈信息。为了更好地了解运营及操作情况，通过集成的日志审计，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，事后审计分析可以帮助管理员快速定位到安全问题。在系统管理方面，支持客户端配置、授权配置、客户端更新、第三方同步配置、应用适配管理等功能。

在办公室访问互联网应用时，通过国密通道来保障网络安全。对于那些潜

在风险的应用或涉密应用，通过云隔离平台来支撑在信创替代过渡阶段访问传统 B/S 和 C/S 应用的工作需求。云端大脑可以判断目标网站是否安全，是否有恶意软件等安全问题。对于远程访问，通过浏览器集成的 SDP 客户端接入来实现统一身份认证，以防范黑客入侵的危险行为。

最后，企业浏览器可以对操作行为进行严格管控。例如，用户在下载文档时，进行在线预览，以确保数据安全。这样，企业浏览器不仅提供了便利性，同时也最大限度地保障了用户的数据安全。

数世咨询认为，企业浏览器通常具备以下核心功能：

3.1 兼容适配

企业浏览器采用了双核架构设计，可以同时运行多种业务，满足不同的使用需求。它还具备多个 JS 引擎和文档模式自动适配功能，能够根据不同应用程序和操作系统的要求进行适配。此外，企业浏览器采用跨平台适配技术，支持 windows 平台、信创系列操作系统平台、Mac 平台，可以抹平不同操作系统和设备的差异性，确保用户在任何设备上都能获得一致的浏览体验。

企业浏览器不仅需要支持主流的应用程序和操作系统，还需要兼容企业内部的各种应用程序，包括历史遗留的应用程序，以确保各种应用程序在浏览器上稳定运行，业务系统正常使用。

3.2 统一管理

企业浏览器拥有强大的管理平台，可以对组织、应用、兼容性、策略、准入、运维等进行全面管理，支持由管理员统一下发配置到员工的浏览器客户端中，进行统一访问策略、统一版本管理、统一应用入口管理，可以让用户轻松访问和管理各类应用，提升工作效率。

此外，它还支持单机和分布式两种部署方式，为业务提供更多灵活性。可

以轻松地控制浏览器的各种设置，并确保其安全性和稳定性，以满足业务需求。

3.3 安全防护

安全防护是企业浏览器核心功能之一，首先安全产品 / 组件集成功能，可以集成防病毒、恶意 URL 检测、终端安全 SDK、SDP 安全远程办公、文档安全、企业 IM 通信、单点登录、身份认证等；其次是安全访问控制，终端访问时通过零信任网络和多重身份验证机制，实现 WEB 访问控制，保障业务系统安全，避免黑客仿冒账号、密码盗用等入侵导致的数据泄露；最后是数据安全防护，对上网行为管控，操作行为的安全审计、敏感信息水印防护，敏感文档数据仅支持在线预览，避免截图等数据泄密行为，对高密业务、敏感文件、研发代码等数据，通过 RBI 技术隔离平台进行防护，退出浏览器时，清空浏览记录，能够实现浏览器全生命周期的安全防护。

3.4 零信任网络访问

对于远程办公访问私有应用，传统方式是采用 VPN 方式，已无法满足当前安全挑战，基于“零信任”安全理念的 SDP 架构，通过将所有应用隐藏，访问者不知道应用的具体位置，同时所有访问流量均通过加密方式传输，并在访问端与被访问端之间点对点传输。与终端环境感知能力协同，能够实时监测终端环境变化、动态调整访问权限，来有效解决企业业务拓展中的安全问题，成为了零信任理念的最佳实践之一。

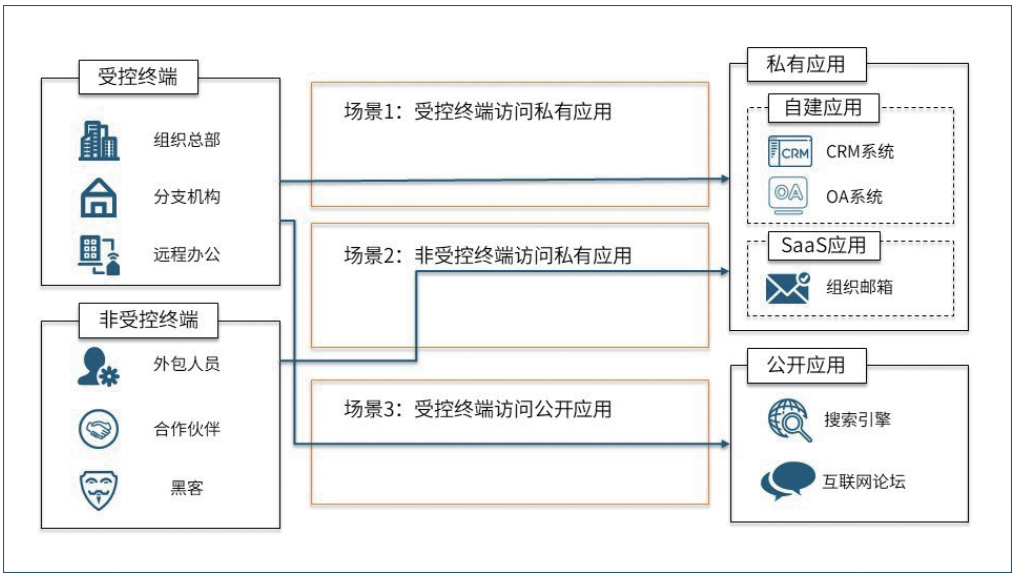
企业浏览器通过集成 SDP 模块，通过身份 / 设备身份验证后，便可直接在互联网中远程安全访问原有的内部业务应用，数据链路全程使用国密算法、国密证书的保护，并支持设备排他性验证，既保证了远程办公的效率，又确保了公司数据安全。

对于办公访问互联网应用场景，员工自身无法判断互联网上的诸多网站是否安全，当访问到“恶意网站”时，网站里包含的病毒木马便会利用系统漏洞入侵系统，因此企业浏览器需要具备风险网址拦截的功能。同时，员工对高密

业务、敏感文件、研发代码等访问时，通过企业浏览器集成的云隔离平台，实现业务、数据隔离不落地访问，将用户的设备 / 网络与 web 代码执行环境之间建立一个安全隔离带，保护关键业务免受攻击。

4、安全访问场景

根据员工终端的位置和属性，数世咨询将浏览器分为受控终端和非受控终端，将访问应用分为私有应用和互联网公开应用，共梳理出三个安全访问场景，如下所示：



安全访问三大使用场景

4.1 场景一：受控终端访问私有应用

针对受控终端访问私有应用场景，组织总部、分支机构、远程办公均有访问私有应用（OA 系统、CRM 系统、企业邮箱等）需求，可以部署企业浏览器并集成防病毒、终端环境感知、零信任网络访问三个模块安全能力。防病毒模块具备多个杀毒引擎，可以对多种病毒进行体征提取、大数据查杀；终端环境感知模块可以对注册表、网络、进程全面动态感知；零信任网络访问模块，通过最小权限控制和持续信任评估，实现动态访问控制，自动策略下发，风险访问处置，恶意行为阻断等，实现随时随地的安全访问。

4.2 场景二：非受控终端访问私有应用

针对非受控终端访问私有应用场景，主要是指外包人员、合作伙伴、黑客，可以部署企业浏览器并集成终端环境感知、零信任网络访问两个模块安全能力。终端环境感知模块可以对注册表、网络、进程全面动态感知，阻断未授权浏览器客户端访问，当终端环境可信度低时，降低访问权限，终端环境发生改变时，重新信任评估；零信任网络访问模块，通过最小权限控制和持续信任评估，实现动态访问控制，自动策略下发，风险访问处置，恶意行为阻断等，实现可控的外来安全访问。

4.3 场景三：受控终端访问公开应用

面向受控终端访问公开应用场景，组织总部、分支机构、远程办公均有访问公开应用（搜索引擎、互联网论坛、主流网站）需求，可以部署企业浏览器并集成防病毒、威胁情报两个模块安全能力。防病毒模块具备多个杀毒引擎，可以对多种病毒进行体征提取、云端大数据查杀；威胁情报模块，具有漏洞情报、API 情报、运营情报、资产情报、恶意网站库等资源，实现外网应用的安全访问。

5、业务场景分析

随着组织数字化转型推进，国内 TO B 行业对企业浏览器的接受度日益提高。这种趋势最直观的体现就是越来越多组织愿意为安全访问进行付费，即采购企业浏览器。

当然，这一现象也得益于信息化、数字化和 Web 化的快速发展趋势，使得办公场景中 Web 应用的占比极大，企业浏览器俨然成为操作系统之上的操作系统。如果企业浏览器能够确保稳定运行、性能优越、并具备统一管控能力，同时能够叠加安全场景，保障办公体验、效率和数据安全，那么它将会获得越来越广阔的发展空间。

基于此现象，数世咨询调研了大量国内企业浏览器付费应用案例，并做出分析：

提升办公生产力，保障业务连续性

应用场景

- 业务系统繁多；
- 依赖IE浏览器各版本；
- 浏览器配置繁琐；
- 插件驱动安装繁琐。

需求痛点

- IE停服问题；
- 一终端多浏览器困扰；
- 浏览器崩溃频繁、办公效率低、运维成本高。

能力展现

- 跨平台支持能力；
- 浏览器双内核支持能力；
- 页面兼容性问题检测及修复方能力；
- 浏览器及相关配置项统一分发能力；
- 插件预装及统一分发能力；
- 具备排障和运维管理能力。

相关案例

政府机构、部委、金融机构（包含银行、保险、证券、交易所等）、公检法司、军工集团、大型能源央企（包括电力、石油石化、华能、核工业等）等客户在应用场景和需求特点等方面具有极高的相似性。

以构建标准，满足合规为目标

应用场景

- 信创迁移适配、国密算法改造、办公软件正版化等合规场景；
- 满足国资委79号文、44号文、36号文、密码法、关基测评等政策法规的要求。

需求痛点

- 业务系统迁移工作量巨大；
- 无统一Web建设标准；
- 国密传输加密需求；
- 办公软件商业授权。

能力展现

- 提供内核稳定的统一浏览器基座；
- 产品具有正规的商业授权机制和配套服务（如版本升级、漏洞修复、定制化服务、技术支持响应服务等）；
- 适配信创生态链，提供完善信创迁移解决方案；
- 具备国密算法支持能力，国密软硬件兼容适配能力。

相关案例

目前主要客群：党政、电信、交通、电力、石油、航空航天行业、教育、医疗行业；长期来看，汽车、物流、烟草、电子等N个行业会逐步发力。在应用场景和需求特点等方面具有极高的相似性。

注重用户体验，满足业务融合需求

应用场景

- 注重终端用户体验；
- 高效运维；
- 数据运营；
- 要求浏览器提供与业务场景深度融合的服务。

需求痛点

- 业务系统跳转逻辑复杂；
- 账号重复多次登录；
- 无统一门户；
- 有统一门户但无统一访问入口。

能力展现

- 多业务系统的兼容能力；
- 与SSO整合能力；
- 与AD域、CAS、LDAP等认证源的打通能力；
- 接口开放给第三方的能力。

相关案例

各类金融机构、大中型央企、民企在应用场景和需求特点等方面具有极高的相似性。

高度数字化业务，保障业务安全性

应用场景

- 关注浏览器自身安全；
- WEB访问安全、身份安全；
- 用户行为安全、数据安全；
- 轻量级的统一访问安全方案。

需求痛点

- 浏览器被恶意进程注入、频繁漏洞威胁；
- 终端环境不安全，业务访问无边界，用户身份不验证，通信链路不加密；
- 用户操作无管制、互联网下载无防护、Web数据泄露。

能力展现

- 完善的浏览器自身安全集成能力（如终端环境安全检测、恶意网址拦截、及时的漏洞修复机制等）；
- 与SSL应用安全网关、身份认证源的整合能力；
- 浏览器操作管控能力（如复制、截屏、上传下载、打印、查看源代码等）；
- 用户行为审计能力。

相关案例

信息化运用发达的企业，预防数据泄露，保护数据资产，主要以民企为主（如开放互联网访问的国企、民企，如金融交易机构、教育机构、审计行业、税务行业、医疗机构等）。

6、市场概况

数据研究机构 statcounter 发布了中国 PC 端浏览器在 2023 年 8 月份的最新数据统计，Chrome 浏览器以 35.12% 的中国份额稳居第一，Edge 浏览器占 22.73% 排第二，360 企业安全浏览器以 18.75% 排第三，Firefox 以 5.22% 排第四，Safari 以 4.17% 排第五。

国内企业浏览器市场，由于 IE 停服、信创替代、等保、密评、数据安全等多重因素的推动，国内企业浏览器市场呈现出快速发展的态势，这吸引了安全厂商、操作系统厂商、公有云厂商、互联网厂商等纷纷进军企业浏览器市场。目前，已经有数千家组织机构（党、政、军、企）落地企业浏览器，解决了 IE 多版本带来的兼容性等难题，实现了跨平台兼容适配、统一管理、安全防护、数据安全等核心诉求。

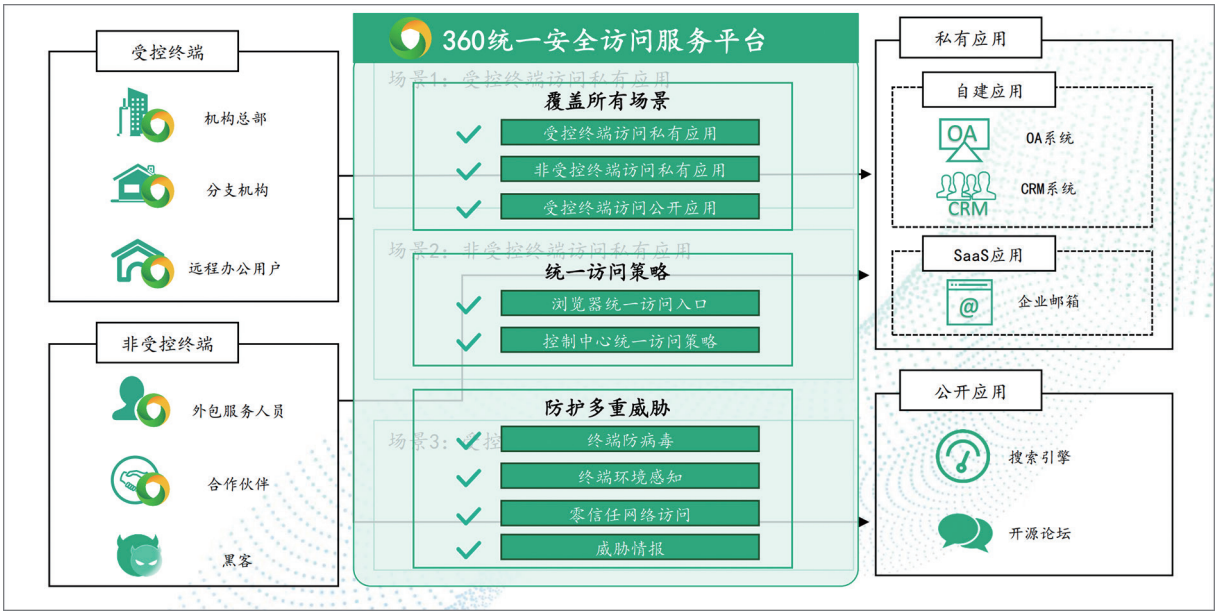
据数世咨询统计，目前，中国企业浏览器市场的规模约 2 亿元左右，市场进入高速发展期。从市场份额和用户量来看，360 数字安全凭借多年投入和积累，在浏览器市场上取得了最高的市场占有率。

随着企业浏览器不断集成安全能力和生产力工具，未来将与虚拟桌面基础设施（VDI）、远程浏览器隔离（RBI）、零信任网络访问（ZTNA）、云访问安全代理（CASB）和安全 Web 网关等技术形成竞争。数世咨询研究显示，随着企业浏览器的不断演变，未来几年将呈高速发展态势。

6.1 360 数字安全

360数字安全
数 字 安 全 的 领 导 者

作为国内最早同时涉足互联网与安全防护的厂商之一的 360，浏览器产品经过 16 年的持续投入与积累，目前 360 基于企业浏览器打造统一安全访问服务平台，通过集成多种安全能力和产品，可以覆盖所有业务场景，同时采用统一访问策略来管理访问权限，从而防护多种威胁和攻击。



360 企业安全浏览器通过统一的部署，构建客户端－控制中心－网关的零信任网络架构，保障全场景的安全访问。

同时，通过将应用访问安全，与业务、身份、权限的深度融合，基于企业级浏览器可以集成多种安全能力和产品，例如，终端安全 SDK、连接云（SDP

客户端）、云盘、BDR、云端安全大脑、360 织语（IM 即时通信工具）等，可以帮助组织建立四大安全访问能力，保障安全场景安全访问，实现业务的高效稳定运行。

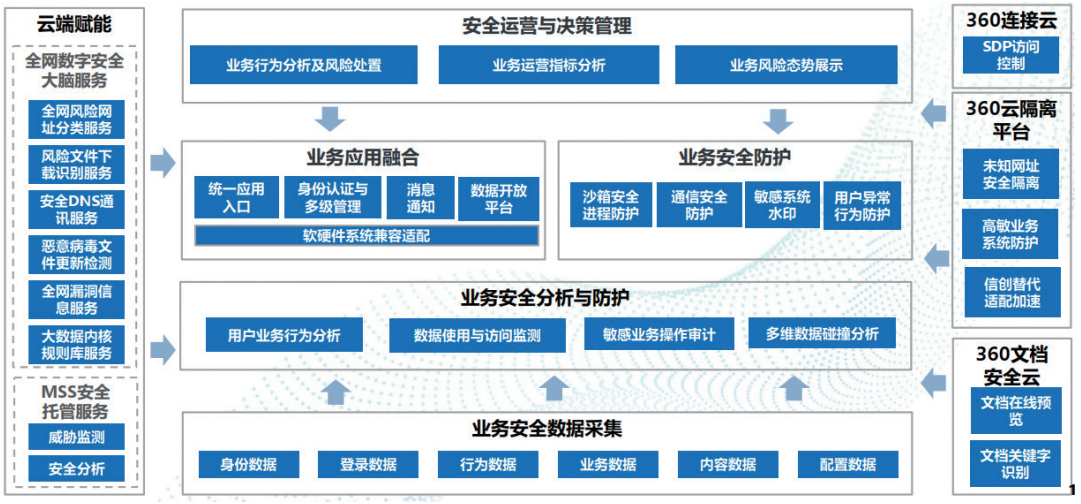
- 统一安全访问策略，统一客户端，统一应用访问入口，统一访问策略，降低黑客利用应用缺陷攻击业务的可能性。

- 增强身份认证能力，浏览器客户端作为唯一业务访问入口，结合企业认证系统，实现增强型身份认证。

- 全生命周期安全防护能力，从启动浏览器开始工作，到业务访问结束退出浏览器，在接入管控、传输安全、数据防泄密、威胁发现等重要场景提供全生命周期的安全防护。

- 简简化安全运行维护，跨平台管控，支持多平台统一管控，统一升级、集中配置下发；支持兼容配置统一下发，配置可信站点管理、弹出窗口管理、插件分发管理、扩展加载管理等；统一访问策略，对接统一身份认证，分权分级管控，运维高效有序，支持单点 / 全局问题修复，避免重复问题处理。

此外，与谷歌、Talon 相比，360 企业安全浏览器解决方案最大的特点是符合国内用户的使用场景需求。



首先企业浏览器采用双渲染引擎（浏览器内核）、多 JS 引擎，自动适配老旧应用平台，实现 B/S 业务系统信创迁移；支持 Windows 平台、Mac 操作系统、信创系列操作系统，给用户带来一致性体验，并与信创生态链中的 200+ 应用进行适配，构建统一应用访问入口，配置参数的全自动化设置，业务系统消息的智能推送。

其次浏览器管理方面，跨平台多设备统一接入管理，精细到用户 / 设备的统一管理，多级管理员 / 多角色分级管理，丰富的 JS API 及系统 API、支持多协议组织架构同步，身份认证对接、SSO 登录融合、SDP 客户端融合、IM 消息融合、云盘功能融合等多项功能。

此外，安全防护方面，依托 360 全网数字安全大脑的深度赋能，在浏览器运行前、中、后期，能够有效应对运行环境受到威胁、浏览器文件受到篡改，浏览器被其他程序调试等安全风险，构建全生命周期的安全防护。360 积极参与 CA/Browser/W3C 国际组织成员、RSA/ 国密根证书计划等，全面参与制定和推行世界互联网标准。

可以看出，作为入选本报告企业代表之一的 360 数字安全，其企业浏览器更加符合本报告“关键能力”部分所提出的跨平台兼容适配、统一管理、安全防护等方面的描述。

官网：https://browser.360.net/

6.2 谷歌

Google

谷歌于 2008 年发布 Chrome 浏览器，经过不断迭代升级，成为目前最流行的浏览器。在 2019 年，谷歌发布了 Chrome 浏览器云管理产品，IT 人员可以

通过管理控制台对组织中的浏览器进行集中管理，包括统一策略管理、浏览器管理（版本、设置、设备详细信息）、安全防护（密码安全、网站安全、恶意软件下载 / 上传）、拓展管控和插件管理，可以对内部 IT 服务的无代理和无 VPN 访问。

为了加强 Chrome 安全性，谷歌又发布了 BeyondCorp Enterprise，这是谷歌自主开发的零信任服务，具有零信任访问、高级可见性、威胁防护和数据防泄露等功能，该服务由身份感知代理（IAP）、身份和访问管理（IAM）、访问上下文管理器、端点验证四个核心组件组成，与 Chrome 集成并提供额外的安全企业浏览功能，可以实现内容传输数据防丢失、高级恶意软件和勒索软件防护、实时 URL 检查和网络钓鱼防护、SaaS 和 Web 应用程序的上下文感知访问等功能。

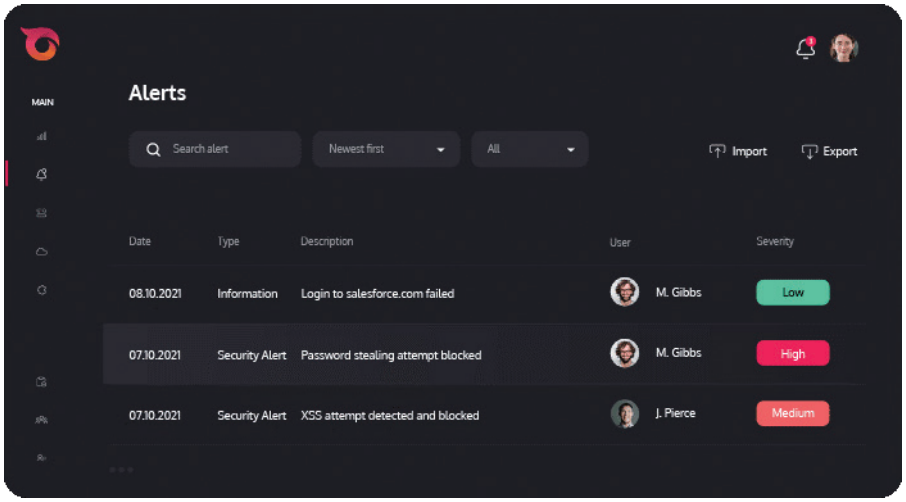
官网：https://chromeenterprise.google/browser/security/

6.3 Palo Alto（Talon）

TALON

Talon Cyber Security（以下简称 Talon）是为远程办公场景提供网络安全解决方案的供应商，旨在保护任何用户、任何设备（Windows，Mac，

Android 和 iOS）、任何位置和任何 Web 应用程序的安全，曾斩获 RSAC2022 创新沙盒冠军。



Talon 的主打产品是一款面向企业的企业浏览器 TalonWork，这是一款基于 Chromium 内核的产品，注入了高级安全功能，专为现代 Web 应用程序和远程用户而设计。Talon 浏览器将浏览器转变为安全的工作空间，为企业 IT 和安全团队提供对所有 Web 服务和用户操作的深入可见性和严格控制，同时为最终用户提供熟悉的体验。

Talon 扩展可轻松安装在任何 Web 浏览器上，帮助企业实现对所有托管设备的可见性和安全性的解决方案。该扩展可作为传统 Web 安全解决方案的替代方案，或作为分阶段向企业浏览器推出的一部分，TalonWork 仅支持本地单机部署方式。Palo Alto Networks 高价收购了 Talon Cyber Security，可见企业浏览器已经成为各大安全供应商重点关注领域。

官网：https://talon-sec.com/technology/

7、未来发展趋势

7.1 企业浏览器时代即将到来

随着浏览器承担工作越来越多，浏览器成为统一访问入口，其安全问题也成为所有组织的关注点。由于业务数据往往具有高度敏感性，政企单位率先采取行动，从浏览器的安全入手——引入企业浏览器。在这个过程中，安全问题成为他们必须面对的关键挑战。为了保障信息安全，政企单位需要选择更加安全、可靠的浏览器。

7.2 AI 工具助力组织提升生产力

随着 ChatGPT 的火爆，以浏览器为中心的 AI 开发工具层出叠现。微软 Edge 浏览器内置了 GPT-4，用户可以在浏览器上点击 Bing 聊天，实现生成式 AI 对话。360 智脑大模型面向公众开放，用户可通过 360 浏览器智脑版体验多角色、多轮对话、AI 工具等特色功能，这种 AI 助手以其出色的智能化、便利性和高效性，正在逐渐改变我们的工作方式和生活方式。

AI 助手和企业浏览器的结合，既保护了用户隐私和安全，又带来了更高质量的生产力提升。随着技术的不断创新和应用场景的不断拓展，AI 助手和企业浏览器的发展将更加紧密地联系在一起，为组织创造更多便利和价值。

7.3 企业浏览器将集成更多安全产品

随着网络攻击手段的不断升级，企业浏览器需要不断强化自身安全能力以防范各类威胁。目前，许多企业浏览器都在集成各种安全能力，包括安全认证、隐私保护、身份验证和访问控制等功能。例如，360 企业安全浏览器采用了先进的防火墙技术来阻止恶意软件的入侵,同时还有插件可以增强对隐私信息的保护，如自动删除浏览记录、阻止追踪等。

北京数字世界咨询有限公司（以下简称数世咨询）是国内数字产业第三方调研咨询机构，主营业务为网络安全产业领域的调查研究、资源对接与行业咨询。在国内网络安全产业的调查研究领域，无论是专业性还是资源丰富性，均处于业界领先地位。

调查研究方面，撰写发布过《中国数字安全大事记》、《中国数字安全能力图谱》、《中国数字安全 100 强》、《中国数字安全产业统计》等业内影响力巨大的公开报告。同时，还为监管机构、国家部委、大型国企等单位提供各种定制化的内部调研报告。

资源对接方面，数世咨询目前已对接国内网络安全企业 700 余家，以及 150 余家有网络安全投资业务的资本方，建立了频繁且良好的沟通合作关系，包括共同举办会议活动，投融资对接，安全产品与企业推荐，企业资源整合等。

行业咨询方面，经常性的为监管部门、国家部委、安全企业、安全用户、一二级市场投资机构提供建议、企业培训及专家评审等咨询服务。

公司地址：北京市东城区鲜鱼口街 90-2 号网安小酒馆
官方网站：www.dwcon.cn
联系邮箱：dw@dwcon.cn

小酒馆

数世咨询

Digital World Consulting

数字安全领域独立第三方调研机构