奇安信可信浏览器

产品白皮书

奇安信集团

2020 年 8 月

版权声明

目 录

第 1 章 背景 1

1.1 浏览器兼容性问题 1
1.2 问题的碎片化与重复处理问题 1
1.3 访问通信安全问题 2
1.4 内部数据揭露的风险 2
1.5 办公场景中的安全如何保护问题 2

第 2 章 产品概述 4

2.1 产品定位 4
2.2 设计思想 4
2.2.1 兼容性和重复劳动解决方案 4
2.2.2 客户端安全解决方案 5
2.2.3 企业数据安全解决方案 5
2.3 产品架构 5
2.3.1 控制中心 6
2.3.2 客户端 6

第 3 章 产品功能 7

3.1 统一办公管理 7
3.1.1 手动创建部门及用户 7
3.1.2 自动同步企业组织结构数据 7
3.1.3 统一的办公入口 7
3.1.4 客户端统一升级 8
3.2 业务兼容 8
3.2.1 内核自动切换 8
3.2.2 IE 可信站点配置 9

3.2.3 弹出窗口设置 9
3.2.4 插件管理 9
3.2.5 配置参数沙箱 9
3.3 统一安全管理 10
3.3.1 安全管控策略 10
3.3.2 客户端安全保护 10
3.4 国密通信支持 11
3.5 信创平台支持 12

第 4 章 产品优势 13

4.1.1 自主可控度高，问题排查能力强 14
4.1.2 多层安全防护，立体保护 WEB 应用安全 14
4.1.3 全面支持国密证书、双向认证功能 15
4.1.4 个性化功能丰富 15

附录： 关于奇安信 2

第1章 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 浏览器兼容性问题

众所周知，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，比如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等。对于普通用户来讲，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。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。而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 问题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，我们保守的推算一下：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，国产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，是国产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国产密码算法，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国产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 Verizon（威瑞森）发布的《2017 年数据泄露调查报告》中可以看到，近 1/4 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 办公场景中的安全如何保护问题

在整体安全防护体系的建设过程中，任何相关角色的安全短板都可能导致整个安全体系的坍塌。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，如何在整个工作生命周期保护用户信息数据的安全性，成为了企业浏览器产品选型过程中的一个重要考量因素。

第2章 产品概述

2.1 产品定位

奇安信企业浏览器是一款以浏览器为载体，面向政企单位，以提高整体效率，降低协作成本，保护信息数据安全，支持信创环境为主要目标的统一办公平台。

奇安信企业浏览器以“广泛兼容、多方智能、全面管理、立体安全”为设计理念，基于 W3C 标准和双核技术，能够全面兼容客户的旧业务，并为企业新业务提供后续的兼容性规范。

奇安信企业浏览器根据多年的使用经验，已经形成了智能化切换技术，可以极大地降低使用成本，提高整体办公效率。

奇安信企业浏览器还提供了强大的管理功能，能够通过统一管理控制台，对企业内部所有的浏览器客户端进行统一配置管理、统一行为管理和统一安全管理。

奇安信企业浏览器还提供了几十项安全解决方案，能够从本地安全、通讯安全、上网安全、行为安全、数据安全等五大维度来解决企业安全浏览的问题。

2.2 设计思想

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，奇安信企业浏览器的理念是：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

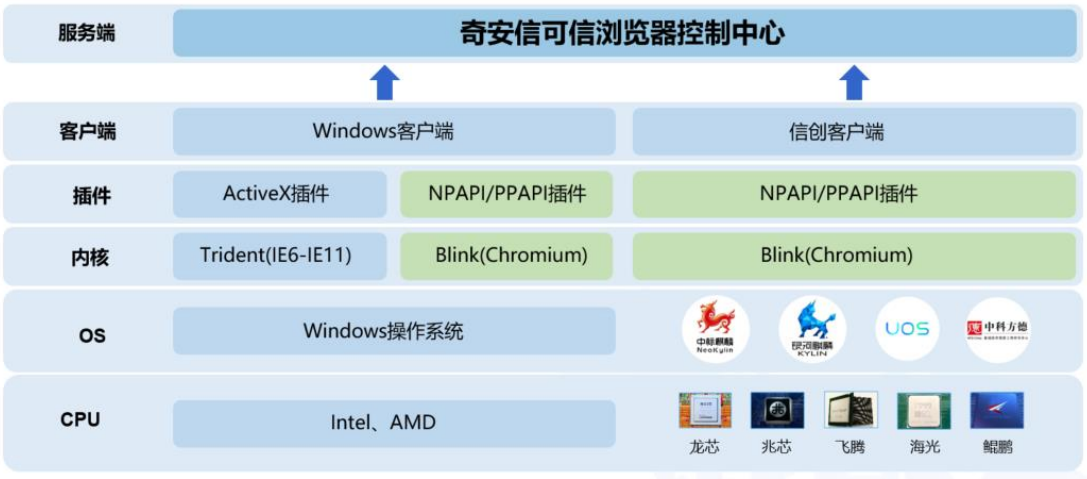
奇安信企业浏览器结合奇安信安全能力，为用户在使用过程中的安全提供各角度的防护机制。比如在使用浏览器访问网站过程中所产生的临时数据的安全保护方案、在需要密码输入环节的安全保护机制、在访问过程中对于恶意网站的防护机制、对于网站证书的安全审计机制、通过浏览器下载文件时的文件安全检测、浏览器所在操作系统的恶意进程监测、对于上网过程中的隐私保护机制和第三方扩展应用的安全审计等各个角度。

2.2.3 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奇安信企业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。

2.3 产品架构

奇安信企业浏览器的产品架构如下图所示：



图：奇安信企业浏览器产品架构

整个奇安信企业浏览器共分为控制中心和客户端两大部分。

2.3.1 控制中心

奇安信企业浏览器控制中心是面向企业 IT 管理员提供的一套企业浏览器集中管理控制平台，为了支持以部门或用户为颗粒度的管理维度的能力，管理后台提供了包括部门及用户的组织结构管理功能。

为了支持由管理员统一来处理兼容性相关的配置问题，提供了由管理员来编写的内核切换策略、IE 可信站点配置、窗口弹出例外策略以及插件管理等功能相关的交互界面；提供了用户行为安全、数据安全保护策略等配置工具来针对需要防止数据泄漏的系统进行安全保护管控。

并针对支持国密加密协议的网站提供相关配置界面，允许浏览器直接以国密加密支持与其建立通讯链接。该管理后台还提供类似自定义首页、扩展管理、消息管理、管理员配置等其他相关的功能，以帮助管理员提供更加全面的管理功能。

2.3.2 客户端

奇安信企业浏览器客户端在启动之后使用之前需要向管理后台提交用户身份信息，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，浏览器客户端的行为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。

奇安信客户端目前支持 Windows 系统操作系统和安可操作系统两大系统操作系统。

第3章 产品功能

3.1 统一办公管理

3.1.1 手动创建部门及用户

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和用户，从模板批量导入用户，并可以对部门及人员信息进行增删改操作，也可以针对人员进行部门调整，权限调整等操作。

3.1.2 自动同步企业组织结构数据

在实际生产环境中，很多企业都会选择使用 AD 或 Ldap 作为用户组织结构和身份认证的管理系统。当企业浏览器作为一套新的业务系统加入到企业的 IT 环境中时，应当允许管理员选择该系统的用户组织结构从统一数据源去获取，而不需要管理员单独去手工创建相应的部门和用户。

奇安信企业浏览器提供 AD/Ldap 组织结构同步配置页面，由管理员填写 AD 服务器的连接及认证方式，浏览器管理后台将根据配置信息去 AD/Ldap 服务器获取相关组织结构和用户数据，并将其保存在本地数据库，管理员可通过部门管理和用户管理模块读取组织结构信息。为了保障 AD/Ldap 数据源的数据变化能够及时同步到浏览器管理服务端，管理后台提供定时数据同步的功能，管理员可配置每隔多久去 AD/Ldap 服务器进行一次数据同步操作。

3.1.3 统一的办公入口

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。

奇安信企业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，用户点击图标便可以直接访问对应的业务应用系统。

3.1.4 客户端统一升级

在企业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。

奇安信企业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。

3.2 业务兼容

3.2.1 内核自动切换

奇安信企业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，所以奇安信企业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，奇安信企业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。

3.2.2 IE 可信站点配置

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，所以奇安信企业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]级别中的多个独立配置项。

3.2.3 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。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。

3.2.4 插件管理

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实现上传、描述及删除功能，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。

3.2.5 配置参数沙箱

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，在奇安

信企业浏览器中是否也会遇到类似的情况呢？这种情况一版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。所以，在奇安信企业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。

3.3 统一安全管理

3.3.1 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。用户行为策略可以限制用户在指定网站内禁止复制数据内容、禁止打印当前页面、禁止将网页另存到本地、禁止使用开发者工具、禁止查看页面源代码、禁用鼠标右键、禁止文件上传动作，全方位保护企业的内部数据资产；而数据保护策略则可以在用户访问特定系统的时候，以页面水印的方式将用户的姓名、手机号、邮箱、当前时间等信息覆盖在当前访问的页面上，防止用户通过截屏或拍照方式泄漏内部数据。

3.3.2 客户端安全保护

- 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，奇安信企业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。

- 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奇安信威胁情报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。

3.4 国密通信支持

奇安信企业浏览器在产品中增加国产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，管理员可以在后台配置支持是否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，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。

3.5 信创平台支持

奇安信企业浏览器全面支持国产系列（包括但不限于龙芯（MIPS）、兆芯（x86）、飞腾（ARM）、海光（X86 AMD））等各架构 CPU；同时支持国产系列操作系统，如中标麒麟、银河麒麟、中科方德等。

第4章 产品优势

4.1.1 体验一致的跨平台技术

奇安信可信浏览器支持了各信创操作系统和 Windows 操作系统。在这些平台上，浏览器是基于同一套代码库的，提供了对 W3C 标准支持的一致性、对流版签等插件接口支持一致性、对扩展接口支持的一致性以及用户体验的一致性。

浏览器一套代码实现跨平台编译，内核一致、平台一致提升开发效率。

使用奇安信浏览器在 WINTEL 终端与信创终端访问业务应用，可获得一致的访问体验。

4.1.2 一体化的安全防护

奇安信可信浏览器与终端安全防病毒系统、电子文件密级标志管理系统和文档发文信息隐写溯源系统协同联动，一体化、多样化、全方位保护企业应用系统及内部数据安全。

浏览器集成杀毒能力，对文件在应用系统内的流转进行安全扫描，提供应用入口的安全保障，避免恶意代码在业务内网扩散传播。

浏览器集成密级标识识别能力，对业务内网中流转的电子文档密级属性自动识别，对电子文档密级和终端密级自动判别，有效拦截低密域对高密域的越权访问，大大降低加密数据泄露风险；自动识别应用系统页面和电子文档的操作属性，根据属性策略拦截对业务数据的复制、打印、保存、查看源代码等敏感行为，同时可设置屏幕水印，全方位保护企业的内部数据安全。

浏览器集成隐写溯源能力，在网页内容中自动嵌入隐写信息，通过截屏、拍照或者打印输出后，图片或者纸质文档依然带有嵌入的隐写信息，可以对图片进行溯源信息提取，可以准确、高效的定位到文

件泄密源头，为保护国家秘密安全提供了一种技术保障。

浏览器集成零信任能力，启动浏览器默认打开零信任 TAC 主页，零信任使用反向代理技术，在 B/S 业务场景下，浏览器支持将应用列表数据导流到 TAP。用户通过浏览器访问应用，如果输入 ip/域名在应用列表中则自动导流到 TAP；如果输入 ip/域名不在应用列表中，再根据访问安全策略判断是否可访问该 ip/域名。

4.1.3 自主可控度高，问题排查能力强

奇安信企业浏览器拥有多年的浏览器研发经验，研发团队均有十年以上浏览器产品开发经验。奇安信企业浏览器团队已经拥有 Blink 内核深度定制能力，能够基于最新版本的 Blink 内核进行开发。

奇安信企业浏览器团队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，并且奇安信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。

4.1.4 多层安全防护，立体保护 WEB 应用安全

奇安信企业浏览器能根据应用的特点，分别提供系统安全、进程安全、内核安全、账户安全、数据安全等 5 个方面的安全防护能力。

- 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。

4.1.5 全面支持国密证书、双向认证功能

奇安信企业浏览器在国产平台上实现了基于国产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。

4.1.6 个性化功能丰富

奇安信企业浏览器具有鼠标手势，收藏夹收藏上万条目录不卡顿，超级拖拽，个性化设置等功能优势：

1) 鼠标手势： 按住鼠标在浏览窗口轻轻一滑，便可快速切换页面，常用功能都能用鼠标手势完成，操作方便，提高办公效率；

2) 收藏夹：可收藏上万条目录及网站，顺畅不卡顿；

3) 超级拖拽：选中链接、图片或者文字，即可拖拽到页面的其他地方进行放置。也可在新标签中打开对应的链接、图片或搜索选中的文字，全面改善传统的浏览体验；

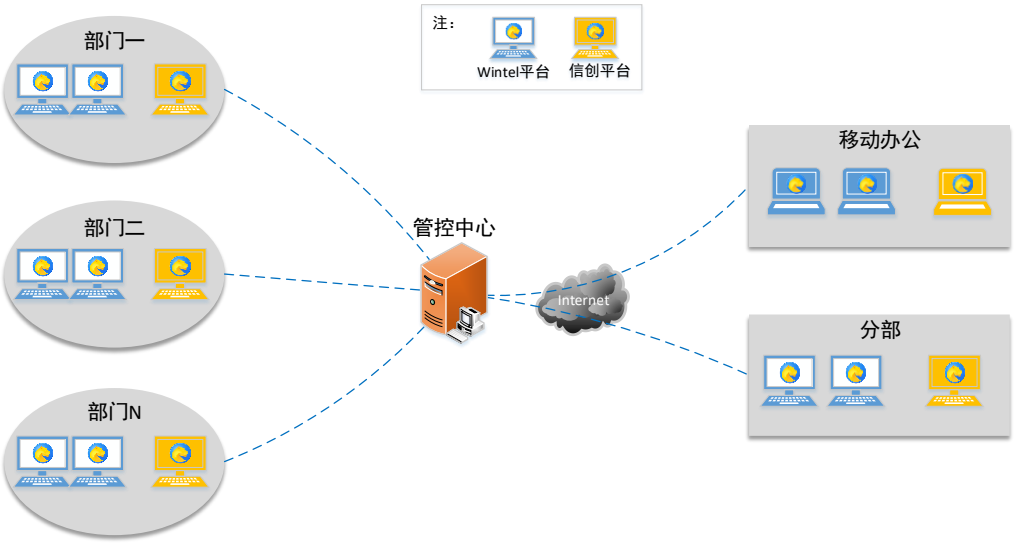
4) 个性化设置：产品界面支持用户个性化定制，可随心设置界面、标签栏、地址栏、搜索栏、网页工具条等；

5) 智能地址栏：可快速补全缓存中的地址，减少 80%的键盘操作，实现网址直达，让操作更简洁。

第5章 产品部署模式

奇安信可惜浏览器的部署分为单机版和管控版，单机版客户端直接在每台终端独立安装部署。

各平台的管控版浏览器客户端，可以通过一个统一的浏览器控制中心来实现信创平台和 Wintel 平台终端的同台管理，管控版的部署模式如下图：



附录： 关于奇安信

奇安信以“让网络更安全，让世界更美好”为使命，以“成为全球第一的网络安全公司”为愿景，不断打造网络安全颠覆性和非对称性核心技术，竞争力不断提高。

奇安信集团（以下简称“奇安信”），是中国最大的网络安全公司之一，专门为政府、军队、企业，教育、金融等机构和组织提供企业级网络安全技术、产品和服务，已覆盖 90%以上的中央政府部门、中央企业和大型银行，已在印度尼西亚、新加坡、加拿大、中国香港等国家和地区开展了安全业务。奇安信的前身为奇安信企业安全集团，2019 年 4 月 30 日更名为奇安信集团。

奇安信是国内网络安全领域中成长最快的企业，拥有近 6000 名员工，2016-2018 年三年的营业收入的年复合增长率超过 90%，增长速度创记录。

奇安信创新实践了新时代网络安全技术发展的“44333”，即四个假设、四新战略、三位一体、三同步和三方制衡：“四个假设”是指假设系统一定有没被发现的漏洞、假设一定有已发现漏洞没打补丁、假设系统已经被黑、假设有内鬼。

“四新战略”是指以第三代网络安全技术为核心的新战具、以数据驱动安全技术为核心的新战力、以零信任架构为核心的新战术、以“人+机器”安全运营体系为核心的新战法。

“三位一体”是高中低三位能力立体联动的体系，低位能力相当于一线作战部队，中位相当于指挥中心，高位相当于情报中心；“三同步”是指同步规划、同步建设和同步运营，提供的是从顶层设计、部署实施到运营管理的一整套解决方案；“三方制衡”是将用户、云服务商和安全公司放在一个互相制约的机制下，第三方安全公司负责查漏补缺，对云服务商形成有力制衡，从最大程度上杜绝漏洞，真正实现长治久安。

奇安信在大数据与安全智能技术、终端安全防护技术、安全攻防与对抗技术、安全运营与应急响应等领域，取得了众多压倒性、战略性的技术成果。公司研发的网络安全态势感知系统，具有全球领先水平，广泛运用到公安、网信等行业监

管和央企、部委的运营监管中，尤其在“十九大”、“两会”等重大会议期间，被有关部门选用于网络安全保卫工作的应急指挥技术系统。在 2017 年爆发的 5•12“永恒之蓝”勒索病毒事件中，网络安全态势感知系统也为公安、网信等领导部门指挥全国应急发挥了重要作用。

在中央军民融合办和军队相关部门指导下，奇安信牵头承建了首个军地联手搭建的“网络空间安全军民融合创新中心”，并和多个军队、军工部门签署了战略合作协议，共同促进网络空间领域军民深度融合。

奇安信的补天漏洞平台，是全球最大的中文漏洞响应平台，拥有 5 万余名白帽子实时提交漏洞，目前提交漏洞数已超过 30 万，成为国家重要机构和企事业单位漏洞响应的保障。

----------End----------