Windows 7 停止服务安全解决方案

地址：北京市西城区西直门外南路26号院1号

Windows 7 停止服务安全解决方案

提要：根据微软官方通告信息，该公司旗下 Windows 7（以下简称 Win7）、Windows Server 2008（以下简称 Server2008）及相关系统已于 2020 年 1 月 14 日正式停止服务，但众多政企单位尤其是关键信息基础设施领域，短期内进行大批量处置存在困难。奇安信集团联合相关操作系统合作伙伴，立足客户切换、升级、过渡三大应对场景和安全运营的长效机制，共同打造安全解决方案，帮助广大客户平稳切换、顺利升级和安全过渡。

本文档帮助您理解停服后客户单位面临的各种风险，以及需要采取积极的措施及处置方法，与合作伙伴共同迈向数字化终端统一安全管理。

关键词：Windows 7 停止服务 Windows 2008 停止服务 Server2008 停止服务 Win7 停止服务

一、 微软：停止支持服务意味着什么

1. 了解微软产品生命周期策略

微软的产品生命周期描述具体到不同产品及版本，给出的政策也比较复杂，但在支持服务方面来说大体有三个阶段，分别是主要支持、外延支持及超出支持。此次 Win7 和 Server 2008 即第二阶段（外延支持）到期。第三阶段超出支持的部分，情况比较复杂，关键基础设施领域相关的客户可以咨询主管部门及网络安全厂商，以便了解相关信息。

根据固定生命周期策略确定的产品生命周期阶段

支持类型	主要支持	外延支持	超出支持终止日期
更改产品设计和功能的请求	可用	不可用	不可用
安全更新	可用	可用	通过扩展安全更新程序提供
非安全更新	可用	通过统一支持提供[1]	不可用
自助支持[2]	可用	可用	可用
付费支持	可用	可用	可用[3]

[1] 通过统一支持提供的外延修补程序支持 (EHS) 计划仅适用于部分产品组。
[2] 自助在线支持在整个产品生命周期内均可用，并且在产品的终止支持后至少能使用 12 个月。提供 Microsoft 知识库文章、常见问题、疑难解答工具和其他资源来帮助客户解决常见问题。
[3] 请转到此处以了解更多信息。需要扩展安全更新程序。

可参考：https://support.microsoft.com/zh-cn/help/14085

另外，各单位通过 WinXP 及 Win7 两次停服事件，应该更加深入理解微软产品生命周期，制定适合本单位使用的处置方案，便于为后续 Win10 及相关产品停服做好准备。更多微软产品生命周期查询请访问：
https://support.microsoft.com/zh-cn/lifecycle/search?alpha=windows%2010

2. Win7 和 Server2008 是主要受影响系统

据微软公告资料显示，截止 1 月 14 日停服的系统包括 Win7 及 Service Pack 版本，Server 2008 及 R2、Service Pack 版本、相关基于该产品构建的其他产品版本，Exchange Server 2010。以应用面较广的前两个系统为例，微软给出的官方说明如下：

1. **Win7 Service Pack 相关版本** 在 2020 年 1 月 14 日之后，运行 Windows 7 的电脑将不再收到安全更新，也不再受到 Microsoft 客户服务提供的 Windows 7 技术支持。随着时间推移，相关的 Windows 7 服务（例如部分游戏、系统周边软硬件）也将停用。详见附录 2；
2. **Server 2008 R2 及 Service Pack 相关版本** 在 2020 年 1 月 14 日之后，Windows Server 2008 和 Windows Server 2008 R2 客户将不会再获得免费本地安全更新、非安全更新、免费支持选项和在线技术内容更新。详见附录 4；

此外，在 2020 年即将停止服务的系统还包括：

产品：	支持截止日期
SQL Server 2008 和 2008 R2*	2019 年 7 月 9 日
Windows Server 2008 和 2008 R2*	2020 年 1 月 14 日
Exchange Server 2010	
Windows 7*	
适用于嵌入操作系统的 Windows 7 专业版*	
Office 2010 客户	2020 年 10 月 13 日
SharePoint Server 2010	
Project Server 2010	
Windows Embedded Standard 7*	

*这些产品符合 **扩展安全更新计划的条件**。

各系统具体版本见附录，可参考：

3. 您将会在电脑上看到的信息

在受此次停服事件影响的计算机上，系统将弹出如下提示对话框

点击了解更多，系统将弹出描述页面信息，促使用户了解相关信息并做出应对措施。

微软称，从 2020 年 1 月 15 日开始，将显示一个全屏通知，说明在 2020 年 1 月 14 日支持结束后继续使用 Windows 7 Service Pack 1 的风险。 该通知将一直保留在屏幕上，直到你与其进行交互。 此通知将仅出现在以下版本的 Windows 7 Service Pack 1 上：

- 入门版。
- 家庭普通版。
- 家庭高级版。
- 专业版。 如果你已购买扩展安全更新 (ESU)，则不会显示通知。 有关更多信息，请参阅如何为符合条件的 Windows 设备获取扩展安全更新和生命周期常见问题解答 - 扩展安全更新。
- 旗舰版。

注： 该通知不会显示在加入域的计算机或处于展台模式下的计算机上。

这个全屏通知中包含的主要信息：

Windows 7 支持将于 2020 年 1 月 14 日终止，如果在支持于 2020 年 1 月 14 日结束后继续使用 Windows 7，电脑仍可正常工作，但微软将不再提供安全更新，不再提供软件更新，不再提供技术支持，这意味着您的计算机将更容易遭遇安全风险。

4. 请尽快安装 1 月 14 日补丁包

事实上在停止服务的当天，微软依旧为 Win7 和 Server2008 推送了一批补丁更新

（KB4534310），本次更新推送了 37 个微软安全补丁，修复了 45 个安全漏洞，其中 8 个微软官方评级为“严重”， 36 个评级为“重要”， 1 个评级为“中”， 这些漏洞影响产品 Windows、Internet Explorer、.NET Framework 和 Microsoft Office，同时推送了 9 个非安全 Office 补丁，请尽快执行 Windows Update 完成补丁安装。

此次更新中请重点关注 Windows 组件 crypt32.dll 漏洞 CVE-2020-0601。 该漏洞可能会对许多重要的 Windows 功能产生广泛的安全影响， 攻击者可以利用这个漏洞，使恶意软件看起来像是由合法软件公司生产并签名的良性程序。 该漏洞影响 Windows 10，Windows Server 2016/2019 版本， 1 月 14 日停止支持的 Windows 7/Windows Server 2008 由于不支持带参数的 ECC 密钥，因此不受相关影响。此次漏洞补丁详细列表见附录 1。

注：**KB4534310** 带来了一些小问题，1 月 31 日又发布了 **KB4539601** 修补这些问题，Win7 仍旧可以安装，但后续补丁则需要购买扩展安全服务 ESU 才可以安装。如果强行安装，系统将会提示，“配置 Windows 更新失败。 正在还原更改。 请勿关闭计算机”，更新可能会在“更新历史记录”中显示为“失败”。

5. 获得 ESU 才可以获得后续更新

据微软公告称，如果您购买了微软扩展安全更新服务 ESU，需要安装如下补丁才可以在 2020 年 1 月 14 日外延支持结束后继续接收安全更新。

a. 在应用此更新之前，你必须安装日期为 2019 年 9 月 23 日的 SHA-2 更新 (KB4474419) 或更高版本的 SHA-2 更新，然后重新启动设备。 如果你使用的是 Windows 更新，则会自动为你提供最新 SHA-2 更新。 有关 SHA-2 更新的更多信息，请参阅针对 Windows 和 WSUS 的 2019 SHA-2 代码签名支持要求。

b. 对于 Windows 7 SP1 和 Windows Server 2008 R2 SP1，你必须具有日期为 2019 年 3 月 12 日的服务堆栈更新 (SSU) (KB4490628)。 安装 KB4490628 后，你必须安装 2020 年 1 月 14 日 SSU (KB4536952) 或更高版本。 有关最新 SSU 更新的详细信息，请参阅 ADV990001 |最新的服务堆栈更新。

c. 对于 Windows Server 2008 SP2，必须安装日期为 2019 年 4 月 9 日 SSU 更新的服务堆栈更新 (SSU) (KB4493730)。 安装 KB4493730 后，必须安装 2020 年 1 月 14 日 SSU (KB4536953) 或更高版本。 有关最新 SSU 更新的详细信息，请参阅 ADV990001 |最新的服务堆栈更新。

详情参考：
https://support.microsoft.com/zh-cn/help/4522133/procedure-to-continue-receiving-security-updates

二、 客户：面临风险及需要考虑的问题

Win7 及 Server2008 是传统 IT 基础架构中的重要组成部分，既承载着业务数据录入、

生产、运营及可视化，也会与各类接口、各类使用者接触，同样影响着最终用户的业务体验，是安全防护的重点对象，也是政企单位网络安全态势感知的基础构成。由于 Win7 和 Server 2008 在国内拥有不小的使用量，且涉及复杂的业务场景及广泛的行业应用，该事件的处置需要进行更为全面的考虑。

1. 系统影响面统计

受此次事件影响的系统在各个行业中占比不小，并且大量业务应用基于这些系统开发，短期内迁移到其他系统的难度极大，因此被攻击的风险会随着停服而加大：

a) **Win7 占比** 市场分析公司 NetMarketShare 数据显示，在 2019 年 12 月，Win7 在全球仍有 26.64%的市场份额。而国内一份统计报告则显示，截至 2019 年 10 月，国内 Win7 的市场份额为 57%。奇安信从**关键信息基础设施行业**客户采样数据观察到，Win7 的存留比例甚至达到 60%以上，部分行业甚至可以达到 70%；

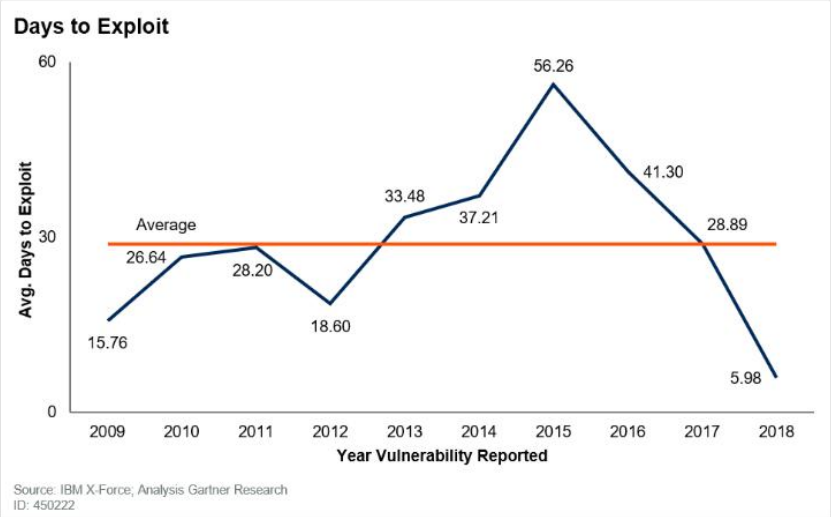
b) **Server2008 占比** 根据 datanyze 的统计数据（采用扫描域名服务统计），中国 Windows Server 占比约为 19.07%，其中 Server 2008 占有率为 15%，而在奇安信椒图事业部的一项抽样调查中（采样约 30 万台服务器）显示，Server 2008 占比高达 27%。

2. 安全风险面分析

1) **近期关键漏洞** 2019 年下半年几乎每个月都有针对 Win7 和 Server2008 的漏洞及攻击出现。其中 BlueKeep 漏洞的影响面巨大，到 2019 年 9 月 7 日，奇安信全球鹰系统评估数据显示，互联网上国内可被直接攻击的受影响 RDP 服务器还有 10 万台量级。停止服务后面临的最关键问题是无法直接获得微软的补丁，一旦出现 Win7 和 Server2008 的相关漏洞，政企客户很有可能在 1 个星期后遭遇相关攻击。同时在一些关基行业的特殊应用场景中，仍旧会有一些系统没有更新最新的补丁，这让攻击者还有可能利用旧的漏洞实施攻击（详见附录 3：Win7 历史上 10 大漏洞及附录 5：Server 2008 历史上 20 大漏洞）；

2) **漏洞蠕虫化** 在攻击形式方面，主要的攻击是漏洞蠕虫化的漏洞，攻击者可以利用这些漏洞，同时结合勒索软件给企业网络造成巨大的损伤。WinXP 停服以后，永恒之蓝勒索病毒在全球范围内爆发，这种攻击形式在 Win7 停服后极有可能再次出现。值得关注的是，最近几年，利用 Win7 系统漏洞正频繁出现。例如，“永恒之蓝下载器”2 小时内便感染超过 10 万用户，爆发力极强。

图2. 从披露开始到被利用的平均时间



3. 国家政策面分析

1) **新基建要求** 从国家部委到各省正在积极推动新基建工程，对相关政企单位尤其是关键信息基础设施领域推动的技术创新及相关数字业务提出了更高的要求，受停服影响的操作系统及应用，将可能影响新基建项目推进；
2) **合规要求** 网络安全法、等保2.0、关基条例、行业规范及实战化演练，主管机构日益重视各单位在网络安全方面的主体责任，受停服影响的操作系统及应用，将影响政企单位的合规性考核。

4. 单位业务侧分析

1) **终端环境复杂** 不同行业的终端类型不同，例如政府金融行业的自助查询终端、制造业的工控终端等，不同安全域的安全等级不同，例如**物理隔离或网闸隔离**，这需要充分考虑单位的管理模式和文化，在确保为终端用户提供良好用户体验的基础上，建设跨类别的数字化终端统一安全管理系统；

2) **单点无法防护** 此次事件并非只是解决 Win7 系统安全的技术问题，而是涉及多行业、多环节、多角色、多场景，处置方案需要融合创新，才能协同共赢；
3) **业务工作影响** 迁移关键业务系统及应用非常耗费时间和金钱，并且可能造成业务中断，政企单位 IT 及网络安全管理者需要进行充分评测迁移计划；
4) **网络安全意识** 受业务工作压力影响，政企单位尤其是关基行业需要进行充分准备才能稳定应对并处置 Win7 停服所带来的影响，在此期间需要强化员工的安全意识，并做好应急预案。

5. 技术支撑层分析

1) **资产盘点及工具选择** IT 管理者需要理清资产，看看有多少关键业务终端以及其他终端的类型及数量，如果只是使用纯粹的 IT 资产管理工具，会使后续的安全加固动作推进困难；
2) **系统关联及工作范围** 由于应用程序、平台及操作系统之间相互关联，IT 管理者可能无法只升级操作系统，而需要对整个系统进行升级，在这个过程中需要嵌入网络安全措施，贯彻三同步原则；
3) **实施经验及安全运行** 各行业 Win7 终端及 Server2008 系统类型繁多，其上承载的业务应用种类繁多，以及各行业数据大集中所带来的架构变化等等因素，相关处置工作并不像封堵某个漏洞那么简单，需要各单位的 IT 管理者具备丰富的实施经验及完善的安全性方案；
4) **漏洞及攻击事件防御** 如前所述，攻击者同样认为停服后一年是个关键时间段，政企单位应该协同国家主管机构及网络安全公司，对停服后 1 个月及半年内，高度关注可能出现的严重漏洞及在野攻击事件，这需要威胁情报平台支撑，同时需要单位自身结合自身业务进行本地化威胁情报生产。
5) **关键技术及内网隔离** 在过渡阶段进行临时加固及防护，需要在底层防护、大规模补丁升级等方面寻求关键技术支持，同时需要考虑到物理隔离及网闸隔离下的检出效率及防护效果。

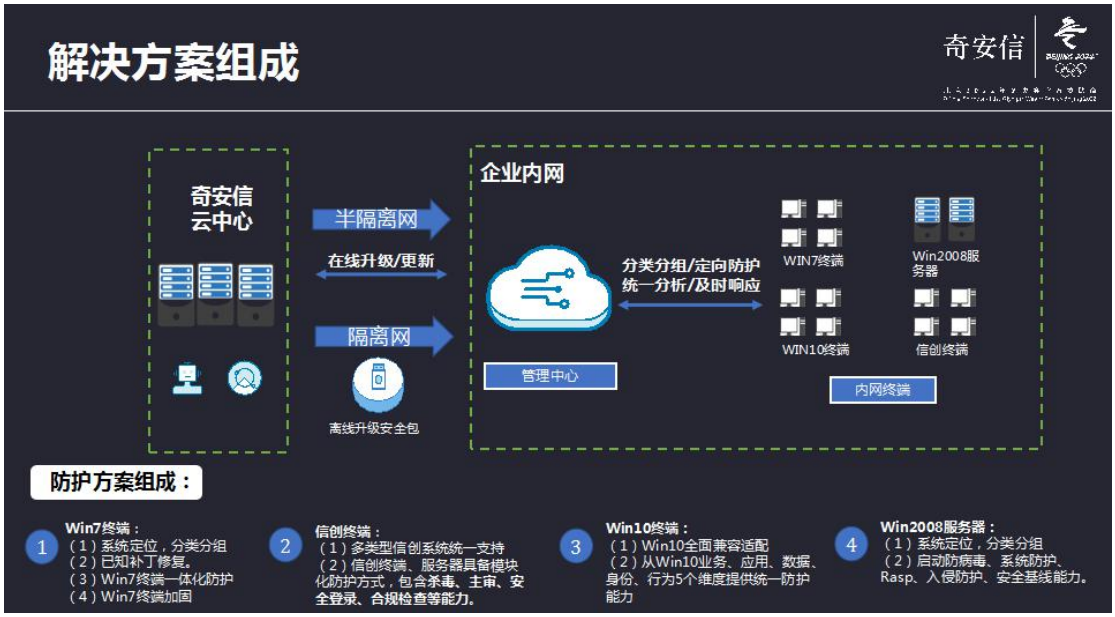
6. 落地实施层规划

各单位需要尽快落实行动计划及实施时间，这需要考虑几个方面：

1) **一处置** 各行业考虑各自业务复杂性，需要圈定实施范围、明确工作阶段，分步骤进行处置动作，或升级或切换等等；
2) **二改造** 未来还有 Win10 和 Server 2019 等系统停服，为避免重复工作，避免 Win7 问题遗留到下一个停服周期，各单位需要适时与信息化及网络安全厂商展开合作，采用先进技术，改造系统架构及安全性，为未来制定长期路线图；
3) **三同步** 以此次事件为契机，政企单位的网络信息化部门应该与网络安全部门携起手来，在 IT 信息化建设与网络安全建设过程中实现同步规划、同步建设、同步运行，尤其是在规划阶段就内建安全能力，为下一停服周期到来争取时间。

三、 厂商：三大场景及长效运营机制

奇安信推出的 Win7 停服应对方案还立足客户切换、升级共三大应对场景和安全运营的长效机制，与产业各界共同打造安全解决方案，涵盖了 Windows 操作系统、信创操作系统、客户端及服务器应用软件等方面，帮助广大客户平稳切换、顺利升级和安全过渡。



1. 过渡：关键技术抵御漏洞攻击

1) **Win7 停止服务的应对措施**

关键技术：奇安信天擎终端安全管理系统提供 Win7 系统加固模块，该模块利用指令控制流检测技术、智能权限分析与设置技术，深入系统更底层，对最先进的恶意软件实施降维打击。这一方案将有效解决系统面临先进的无文件攻击形式时，传统的、基于攻击代码文件特征的针对性 IPS 入侵防御系统方案、临时安全漏洞热补丁方案、针对性 Sandbox 沙箱技术、非白即黑管控方案，防护能力滞后的问题。

视频请访问：https://www.qianxin.com/win7Server2008/

2） 为购买 ESU 的客户提供分发服务

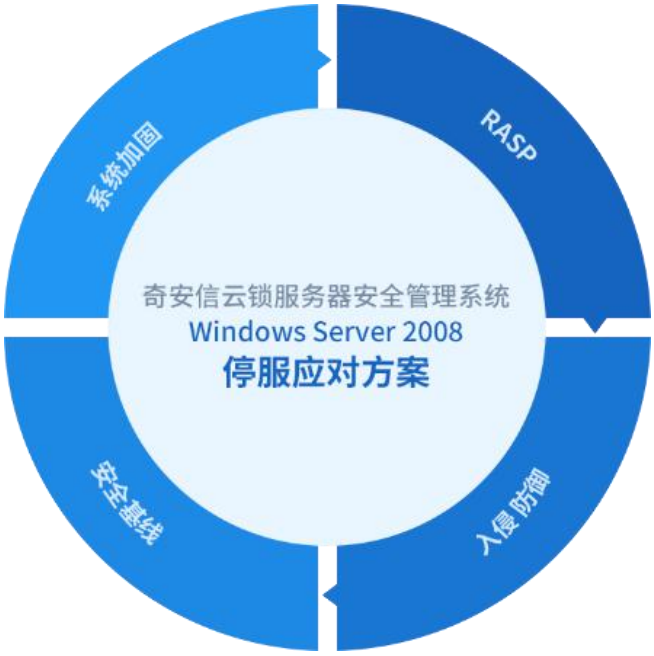
关键技术：如果您获得了 ESU，奇安信可以提供专用补丁库**分发服务**，以便您持续获得安全更新，例如 1 月之后发布的 KB4537820 及 KB4540688 等。 基于奇安信终端安全管理系统，管理员可以通过终端发现模块定义网络 IP 段分组，对指定的网络分组进行周期性地发现（采用多协议、多机制方式）与统计网络中的终端数量及类型。通过该功能，单位管理员可以快速了解全网终端数量及软硬件状态，为补丁分发提供有效的参考。

另外，对单台终端具有全面的安全运维管理功能，包含终端的硬件资产管理、软件资产管理、系统服务管理、进程管理、账号管理、网络管理、系统事件管理、补丁管理及分发、终端安全威胁统等功能，可视化统筹企业终端资产，快速定位终端信息及安全状态。关于奇安信天擎详情请见附录 7。

3） Server2008 停止服务的应对措施

关键技术： 奇安信提供的云锁服务器安全管理系统，基于服务器端轻量级代理，能够安全加固服务器操作系统及应用，融合资产管理、微隔离、攻击溯源、自动化运维、基线检查等强大功能，在国际上率先符合 Gartner 定义的 CWPP、EDR 及 EPP 三大标准要求。解决了传统安全手段在有补丁的情况下，频繁推送补丁影响业务运行；或者无补丁情况下被迫牺牲业务保安全等问题。

奇安信云锁服务器安全管理系统（以下简称云锁，详细介绍见附录 8）正是基于这种攻防对抗理念，通过服务器端轻量级 agent，安全加固操作系统及应用，有效检测与抵御已知、未知恶意代码和黑客攻击，四层防护助您对抗 Windows Server 2008 停服危机。



1） 第一层防护：系统加固，防御漏洞利用行为

漏洞攻击的入口是对外开放端口，而监听了这些端口的进程，则是漏洞攻击的第一个落脚点。云锁通过系统加固功能，将进程的异常行为（黑客利用漏洞后发起的行为）进行了权限限制，例如：“禁止对外服务进程创建可执行文件”，可以有效防御黑客的漏洞利用行为。

系统加固项名称	防护作用
对外服务进程创建可执行文件	限制黑客利用应用漏洞上传或从远程下载后门及提权等程序
对外服务进程执行危险命令	限制黑客利用应用漏洞执行系统命令获取系统信息、添加管理员账户等
对外服务进程执行非正常扩展名可执行文件	阻止黑客通过将可执行文件名修改为 jpg 等扩展名绕过上传限制，然后执行
对外服务进程创建危险扩展名文件	在 Windows 系统上，限制黑客利用应用漏洞上传非 web 类脚本文件，实现白利用
禁止对外服务进程监听原始套接字	限制黑客利用应用漏洞监听原始套接字嗅探网络数据
禁止对外服务进程更改 Linux 系统配置文件	限制黑客利用应用漏洞修改系统配置文件
禁止对外服务进程添加定时任务	限制黑客利用应用漏洞添加定时任务获取执行权限
禁止对外服务进程修改账户信息	限制黑客利用应用漏洞添加管理员账户
禁止对外服务进程修改系统日志	限制黑客利用应用漏洞删除系统日志
禁止对外服务进程运行隐藏的进程	限制黑客利用应用漏洞执行隐藏进程
禁止对外服务进程编译文件	限制黑客利用应用漏洞通过上传源代码的方式，编译出后门文件
禁止对外服务进程修改 SSH 认证文件	限制黑客利用文件上传漏洞修改 ssh 认证文件，进而获取系统登录权限，例如：redis 未授权访问漏洞

2） 第二层防护：RASP，增强应用自我防护能力

云锁 RASP（应用运行时自我保护技术）功能是利用脚本解释引擎（php/java 等）本身提供的插件机制，将具有安全防护功能的插件注入到解释引擎内部，通过在特定的行为监控点上埋点，在应用内部完成对流量、文件、命令执行、数据库访问、网络连接等行为的监控及防护，使应用具有自我防护的能力，能基于行为有效检测已知、未知安全威胁。例如最新曝出的 Weblogic CVE-2019-2725 反序列化 0day 漏洞，云锁无需升级即可防护。

相比传统 WAF 仅仅基于 HTTP 协议流量进行过滤，RASP 除了监控 HTTP 协议外，它可以细粒度的监控应用脚本的行为及函数调用上下文信息，同时支持 T3、JMX 等应用私有协议漏洞的防护。

3） 第三层防护：入侵防御

除了漏洞利用防护外，云锁还提供多维度的服务器入侵防御手段：

- **RDP 暴力破解防护** 防止远程桌面暴力破解；
- **异常登录检测** 针对白名单以外 IP 的登录行为进行告警；
- **远程登录限制** 通过配置登录防护规则实现针对 IP、用户、时间的远程登录限制；
- **端口扫描防护** 针对黑客的端口扫描行为进行识别和阻断；

- **盗取内存密码防护** 针对黑客利用 minikatz 等工具从系统进程 lsass 内存中 dump 登录凭证的行为进行阻止，防止黑客在已攻陷服务器上通过该方式读取到管理员密码后，进而对采用相同密码或者登录凭证的其它服务器进行渗透。

4) 第四层防护：制定安全基线，全方位安全自检

基于云锁的资产管理功能和基线检查功能，可以定制针对 Server 2008 服务器的基线检查模板，从账户、密码、配置文件、权限、服务等多个层面全面自检服务器安全状态。

2. 切换：安全有效的一体化防护解决方案

部分客户正在计划逐步切换非 Windows 操作系统，针对这些系统部署后面临的数据集中、主动防御、协同防御、兼容稳定、统一管理等要求，奇安信网神终端安全管理系统（信创版），已经实现了对飞腾、龙芯、兆芯、申威、海光等 CPU 以及银河麒麟、中标麒麟、中科方德、UOS 等主流国产操作系统的全面兼容适配，该安全管理系统及一体化防护解决方案已经在客户侧投入稳定运行。

3. 升级：安全地升级到最新系统

升级到最新的操作系统是现有 Win7 用户的有效选择，奇安信联合神州网信，为政企客户提供安全无忧 Win7 升级到 Windows 10 神州网信政府版操作系统迁移/升级服务，包含前期规划、升级前评估与应用改造咨询、升级试点验证及大规模部署等内容。在此基础上，奇安信融合了具备集中管理、补丁分发等功能的天擎一体化安全治理框架，从业务、应用、数据、身份、行为 5 个维度，为客户提供安全升级保障。

Windows 10 神州网信政府版是基于最新操作系统技术在国内进行定制开发的安全可控操作系统，面向政府及国有企事业单位用户，基于中国政企客户的应用需求及特点定制开发，满足安全可控需求的操作系统平台，详情请见附录 6。

神州网信建议遵循以下过程，顺利完成迁移与部署工作。

1） 规划

政企用户在进行 Windows 10 神州网信政府版导入之前，需结合自身情况，作好相关准备及规划工作，分步实施、有序推进；分别作好整机预装采购与存量 PC 升级计划。

- 用户场景调研
- 软硬件资产调研
- 确定采购模式
- 升级路线确定
- 部署方式规划
- 部署方案技术论证
- 补丁策略规划

在迁移规划过程中，需要根据客户前期沟通，进行 IT 基础设施调研、IT 基础设施评估等准备，根据有关结果量身指定导入路径。

IT 基础设施调研内容包括：

- 硬件信息（存量机器、外接设备等）
- 软件信息（终端软件、应用系统等）
- 网络架构（AD 域、访问互联网、虚拟环境等）
- 组织架构及人员规模
- 采购模式（OEM、PCIB）

IT 基础设施评估内容包括：硬件兼容性评估、网络环境评估、软件兼容性评估（Win32 程序、IE11 程序等）、域策略兼容评估以及部署规模评估等。

根据以上评估初步定制导入路径，迁移内容计划包括升级策略、部署方式、补丁策略、激活方式等，同时制定升级计划、成立项目组、制订相关人员安排等。根据神州网信有关规划及实施总结主要前期规划内容如下图。

2） 测试

为避免最终用户使用新的操作系统所面临的软硬件兼容性及与当前网络、应用的整合适配，需要制定计划、流程进行全面的兼容性及用户环境测试。

主要测试内容：

- 整体基础架构测试
- 硬件兼容测试
- 软件兼容测试
- 桌面管理类软件测试

详细规划的测试内容包括：整体基础构架需要确定域环境验证（活动目录、组织架构、管理策略）并验证网络环境（网络架构、网络协议、网络服务器等）；硬件兼容性需要测试主机配置标准（存量机器主流型号统计和验证、OEM 新采购机型验证、是否支持指纹识别、是否支持面部识别等），整理外围设备列表（打印机、扫描仪、投影仪、加密狗、读卡器、手写笔/触屏等），同时检查驱动程序证书问题；应用软件的兼容性测试包括：Win32 程序验证、C/S 应用验证、B/S 应用验证；桌面管理类软件测试重点在于：安控软件、杀毒软件、补丁分发软件、CA 认证(USBKey)等。

从 Win7 迁移到 Windows 10 神州网信政府版技术遇到的问题及指导建议如下：

问题汇总	Windows 7	Windows 10 神州网信政府版 迁移建议
硬件问题	OEM 新采购机型评估 存量机器主流型号统计和评估	先评估机器型号是否支持新操作系统
驱动问题	外围设备驱动程序不适用于升级 CA证书不适用于升级	预备驱动程序及证书 逐步淘汰旧的驱动 改造使用开发中的驱动
C/S应用	有些32位的应用不适用64位系统 某些业务或功能无法访问硬件或调用系统接口不成功	建议升级到64位程序或需要对应用的代码进行改造
B/S应用	配置问题需要进行相关设置，如安装ActiveX控件 IE文档模式、UserAgent等问题 B/S应用代码问题	配置问题：通过IE的相关设置，根据应用的提示安装相关证书或ActiveX控件 文档模式问题：通过设置兼容性视图和企业模式解决 B/S 应用问题：修改应用代码

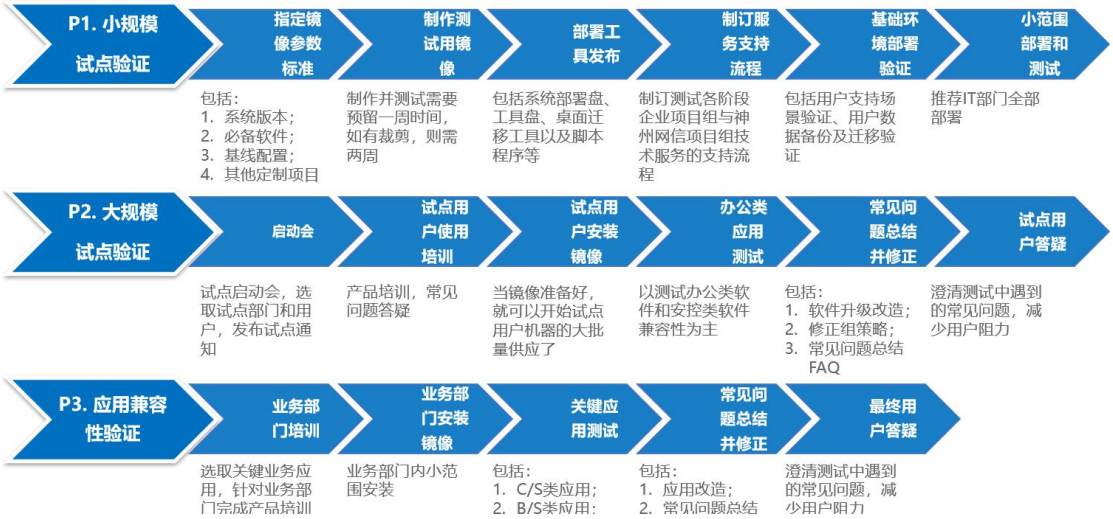
3） 试点

在兼容性改造工作完成后，需按政企用户特点、规模选取代表性用户进行规模化试点，以验证基础环境及应用软件改造效果，使用体验，进行进一步的评估分析，循环改进提升。

- 部署工具发布

- 升级服务器部署
- 制定技术支持流程
- 用户支持场景验证
- 基础环境部署验证
- 用户数据备份及迁移验证
- 应用兼容性用户流程验证
- 试点用户培训

整个试点分三个阶段：P1 小规模试点验证、P2 大规模试点验证、P3 应用兼容性验证，每个阶段由不同的工作任务组成，具体任务列表如下：



4) 部署

在用户规模化试点完成后，分类型、分阶段进行各部门、科室部署，依据政企用户采购方式可以进行整机预装采购或单独操作系统软件采购。

- 修正镜像标准
- 制作标准镜像
- 新机器预装镜像
- 用户数据迁移
- 存量机器升级

部署场景及建议采用的技术方案

- 擦除和加载(Wipe and load)方式
- 就地升级(In-place upgrade)方式
- 预配(Dynamic provisioning)方式

	场景一	场景二	场景三
场景	当需要升级大量应用程序及迁移CMGE操作系统时 当对设备或操作系统配置进行重大更改时 当不需要保留现有应用或数据的情况时 当从未对终端电脑进行有效管理时	当希望保留所有或至少大多数现有应用程序时 当不打算更改： 设备配置（将BIOS更改为UEFI等） 操作系统配置（将x86更改为x64、语言更改、将管理员更改为非管理员、Active Directory域合并等）时	对于新设备，像OEM方式采购新设备时 能自助安装特定于用户或特定于角色的应用的分发工具（Microsoft的WDS、MDT软件等）结合使用时
建议方案	擦除和加载(Wipe and Load)方式	就地升级(In-place upgrade)方式	预配(Dynamic provisioning)方式
方案简要	传统流程： 捕捉数据和设置 部署CMGE操作系统映像 安装驱动程序 安装应用程序 恢复数据和设置 仍然是适用于所有场景的部署选择	让操作系统完成升级工作 保留所有数据、设置、应用程序、驱动程序 安装CMGE操作系统映像 恢复所有内容 建议用于现有设备(Windows 7/8/8.1)	预配新设备 转换为企业设备 删除额外项目，添加组织应用程序和配置 适用于新设备的新功能

5） 优化

在运维优化阶段，除了持续的运维支持外，还要不断优化政企用户内IT环境效能，完成新版本上线和针对最终用户的培训工作，以便从各方面提升用户满意度。

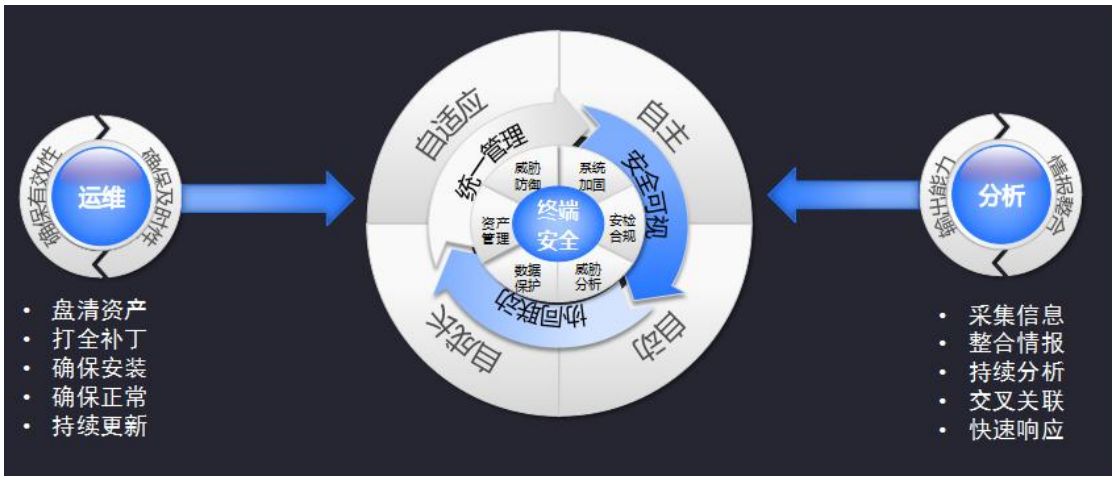
- **IT环境持续优化** Windows 10 神州网信政府版给用户带来更多的基于网络的新功能，及时升级和优化IT环境将会得到更好的用户体验。
- **软件兼容问题追踪** 将用户反馈的软件兼容问题及时反馈给软件厂商并进行追踪。
- **IE兼容问题追踪** 将用户反馈的IE兼容问题及时反馈给网页制作团队并进行追踪。
- **新版本及时上线** 及时将解决了兼容性问题的新版本发布给终端用户将会更好保证日常工作的顺利进行。
- **最终用户宣传** 将新操作系统和新功能及时地宣传给用户，让用户体验到新系统和功能带来的卓越体验。
- **提升用户满意度** 收集用户的反馈信息，分享给软硬件等生态合作伙伴，共同合作提升用户满意度。

表格： Windows 7 升级到 Windows 10 神州网信政府版简要安全及性能对比

		Windows 7	Windows 10 神州网信政府版
安全	Windows更新补丁	2020.1.14 停止操作系统Windows更新补丁	实现操作系统本地补丁更新，国内提供相关服务，国内补丁核查
	激活数据可控性	操作系统激活需要连接境外服务器	操作系统激活在境内完成，激活相关数据不出境，保证政企用户相关数据安全
	遥测数据的可控性	遥测功能相关收集的数据可能同步至境外数据库	遥测数据不出境，保证政府及关键信息基础设施领域用户敏感数据安全
	数据保护	磁盘数据加密保护需要另行选择第三方工具，系统默认无法保障用户数据安全	具备磁盘加密功能，可实现自动化磁盘加密，并整合多项企业级安全特性
	自动化设备安全更新	需手动更新硬件驱动程序以保证硬件设备代码更新以保障其安全性	自动化地更新硬件驱动程序，确保设备安全弱点及时修补
	核心文件保护	采用第三方安全软件先检测后阻止的模型来保证应用程序和核心文件的安全性，但事后检测规则有滞后性，无法防止所有恶意软件攻击	采用设备卫士（Device Guard）的方式对应用程序及代码进行严格检查校验，对重点应用和核心文件进行全方位安全防护
	操作系统全生命周期保护	在开机阶段不能受到保护，系统引导阶段可能已被非法代码感染	安全加载（Secure Boot）功能保护受到UEFI支持，可保障安全地引导操作系统启动过程安全性
	身份认证保护	依赖密码保护，默认策略安全性较为脆弱	根据监管要求加强了密码强度及相关安全策略，提高了系统的整体安全性
性能	最大物理CPU数	2	4
	最大内存	192G	6TB

4. 长效机制：安全运营确保等保合规以及指标考核的完成

终端安全环境的保障是个持续的过程，涉及到很多繁琐的日常工作，面对日益严峻的威胁，极有可能“一失全无”。奇安信针对用户终端安全使用场景，提供一整套完整的量化指标水平服务标准体系，结合多样、细化的流程管理制度，通过经验丰富和数量庞大的运营服务团队+安全分析专家，真正帮助客户扎实、持续做好终端安全的风险监控与修补工作，推动企业终端安全水平提升的年度性运营服务。可以满足上述三大场景下，客户面临的精细化管理、安全管理人员升级、终端安全能力提升及用户体验改善等需求。



四、 迈向数字化终端统一安全管理

2018 年底中央经济工作会议明确了 5G、人工智能、工业互联网、物联网等“新型基础设施建设”的定位，2019 年政府工作报告中表述“加强新一代信息基础设施建设”，2020 年 1 月 3 日国务院常务会议再提新基建。如前文所述，终端上安全能力要求的不断扩展，不单需要覆盖终端自身的安全问题，还需考虑数据中心计算、存储和各类网络服务延伸带来的接入安全、数据安全等问题，关键信息基础设施领域的政企单位在构建全面的、统一的数字化终端安全管理迫在眉睫。

2020 年，各政企单位尤其是关键信息基础设施领域，应将此次 Win7 停服作为一个契机，充分考虑组织的管理模式和文化，推动技术革新及安全能力建设，在确保为终端用户提供良好用户体验的基础上，建设跨类别的数字化终端统一安全管理系统，从容应对新基建乃至数字化转型过程中不断变化的网络安全风险。

1. 在战略愿景方面

1) 坚持“关口前移”思想，构建企业级内生安全体系

在《国家网络空间安全战略》提到“没有网络安全就没有国家安全，没有信息化就没有现代化”。网络安全和信息化是“一体之两翼、驱动之双轮”，这是国家战略层面对安全和

信息化的定位给出了明确的诠释，这要求安全不应以“创可贴”方式开展，要避免碎片化的产品堆砌，安全应该与信息化相互融合、相互影响，形成“DNA 双链”，使安全成为信息系统的一种内在属性而非外挂。

“内生安全”强调安全与信息化的融合。“关口前移”也并不是把防护措施前移，而是安全与信息化做同步规划。以往很多的安全措施失效、安全设备没有发挥作用都是因为没有在信息化建设早期的规划阶段跟安全结合。因此，要解决这个问题就需要通过安全与信息化的同步规划实现安全与信息化的深度结合和全面覆盖，在信息化架构设计时，充分考虑了安全能力的融入层次和集成点，使安全能力得以通过内生方式实现。

2） 重构企业安全架构，促进安全工作在各层次快速达成共识

非网络安全岗位的人员对于安全的理解程度有限，通常只能按照自己的背景知识和经验去理解网络安全，由于安全和信息化融合过程中缺乏专业性、系统性、一致性的语言，这就使得“管业务必须管安全”这句话难以真正落实；也会导致安全防护措施难以形成标准化，有效性不足。

企业通过网络安全规划，将重构企业级网络安全架构，有利于公司网络安全与国家网络安全战略保持一致，有利于公司网络安全战略的落地执行，有利于在企业的各层级、各业务口对网络安全达成一致的理解，这为安全能力的集成与工程落地提供了意识上的广泛共识。

3） 绘制安全体系建设蓝图，勾勒网络安全演进路线

大多数情况，业务人员和安全技术人员因为其关注点不同，对同一安全问题存在不同角度的理解，这对网络安全管控的范围和职责界定有大量的模糊地带，对安全工作造成了很大的障碍。

企业通过网络安全规划，将重构企业级网络安全架构，为企业的 CISO、业务人员和安全技术人员建立共同的蓝图，呈现出未来安全工作全景，使安全技术人员能正确地理解业务需求的同时，又使业务人员能够了解未来信息系统安全实施的全貌，明确了安全和业务之间的工作边界和相辅相成关系。通过安全规划，在体系蓝图之上勾勒出安全演进路线，确保安全工作的落地性。

4） 采用能力导向的网络安全规划方法构建新体系

以往，安全规划大多采用了对标、合规等思想，基本满足了企业的规划需求。但随着威胁类型和强度的增加，传统的规划思想已经暴露出众多的不足，无法用“可确认、可度量”的方式进行威胁控制，即使做了大量安全建设，CISO 们仍然感到心中“无底”，“向上”汇报很难以阐述输出价值，导致安全工作陷入被动。

企业应开展能力导向的网络安全体系规划，重点在于用安全能力框架适配企业安全现状，从而找到深层次的、细颗粒度的安全程度差距，而不仅限于某功能“有没有、做没做”，为实战化的安全体系建设识别需求，使安全能力的有效性达到“可确认、可度量”级别。知道自己能防什么，不能防什么，安全能力底线在哪里。

5） 应对网络安全动态风险，实现实战化闭环运行

网络安全是动态的，企业需要应对技术演进、产品迭代、多源威胁、和监管加强所带来的各类风险。网络安全没有绝对，单纯的人力、物力投入与设备堆砌已经不能适应新时代的网络安全的需求，企业的网络安全体系建设必须面向实战化。

通过安全规划，将运行流程、技术、人和管理规范整合形成一个完整体系，才将能力有效输出。安全运行跟随变化做不同的行动和响应，解决漏洞问题和补丁问题、产品和策略部署调整、威胁的猎杀、事件的监测与响应、情报数据的收集分析和溯源研判，以及安全众测和攻防演习等，使安全与信息化的全面覆盖、深度结合、有效检测、协同响应，最终实现实战化闭环运行。

6） 建立协作、制衡的安全组织，发挥人的关键作用

人是安全的尺度，也是安全运行的关键。如果没有相应的组织机构与人才体系，技术平台无法高效持续运行，安全能力也就无法持续输出。

通过安全规划，将梳理企业在安全机构岗位设置方面存在的不足，有力支撑企业安全工作开展。
首先，应健全安全机构设置。在企业中要建立协作、制衡的安全组织，避免权力过度集中导致的“一点失效，全网贯通”，也要做到“互相监督，群防群治”，通过合理的安全运行流程设计控制错误率，提升运行质量。
其次，应加强人才梯队培养。要明确企业级网络安全人员培养策略，要让具备不同技能的人员参与。要从人的层面入手考虑运行，可以分为安全运营人员、分析响应人员和攻防渗透人员三类，不同人员需要不同的培养体系和培养方式。

2. 在战术执行方面

1） 在终端和周边环境上构建面向终端硬件、操作系统、应用软件、数据资源、用户身份、操作行为和末梢网络的一体化安全技术栈；
2） 制定和落实标准纳管、分权操作、分级管控、集中分析、全局可视的安全运营任务目标；
3） 充分利用终端安全的控制能力和数据资源，实现与企业数据安全、系统安全、身份安全、行为安全等其他安全运营目标的有效衔接和深度聚合。

与IT业务关键聚合点	主要参与方	覆盖面
• 终端派发及BYOD策略 • 操作系统部署管理 • 终端资产及CMDB管理 • 终端远程协助和远程管理 • 办公局域网网络接入 • IT服务台工作流程	• 安全管理部门 • 安全运营部门 • 终端维护部门 • IT 服务台 • 接入层网络维护团队	• 企业所拥有终端，仅用于企业工作目的 业务终端，通常通过专网接入（桌面PC、云桌面） 专用终端，不使用操作系统进行交互（自助服务终端等） • 企业所拥有终端，可用于个人用途 （桌面PC、移动PC、Mobile） • 个人所拥有终端，合规情况下可用于办公 （移动PC、Mobile） • 不可管理终端，属于第三方，但需要网络接入

为有效应对此次 Win7 停服事件所带来的安全风险，请您尽快联系您的奇安信服务人员，或拨打客服电话 +86（10）57836300，以便获取专业见解。如果您需要即刻应对安全事件，请拨打奇安信应急响应电话 4008136360-6

五、 附录

1. 2020 年 1 月 14 日补丁包详细内容

奇安信集团最新补丁库 2020.01.15.1 已发布，本次更新推送了 37 个微软安全补丁，修复了 45 个安全漏洞，其中 8 个微软官方评级为“严重”，36 个评级为“重要”，1 个评级为“中”，这些漏洞影响产品 Windows、Internet Explorer、.NET Framework 和 Microsoft Office。同时推送了 9 个非安全 Office 补丁。

请重点关注 Windows 组件 crypt32.dll 漏洞 CVE-2020-0601，补丁列表见第 2 章。该漏洞可能会对许多重要的 Windows 功能产生广泛的安全影响，攻击者可以利用这个漏洞，使恶意软件看起来像是由合法软件公司生产并签名的良性程序。影响 Windows 10、Server 2016/2019 版本，而于今年 1 月 14 日停止安全维护的 Windows 7/ Server 2008 由于不支持带参数的 ECC 密钥，因此不受相关影响。

如下摘录此次与 Win7 及 Server2008 相关的漏洞信息如下：

KBID	奇安信集团级别	产品	CVE 编号	漏洞的影响	公开披露	已受攻击	最新软件版本	较旧软件版本	拒绝服务

4534314	高危	Windows 7 for x64-based Systems Service Pack 1, Windows Server 2008 R2 for x64-based Systems Service Pack	CVE-2020-0607	信息泄漏	否	否	2	2	N/A
			CVE-2020-0615	信息泄漏	否	否	2	2	N/A
			CVE-2020-0608	信息泄漏	否	否	2	2	N/A
			CVE-2020-0611	远程执行代码	否	否	2	2	N/A
			CVE-2020-0620	特权提升	否	否	2	2	N/A
			CVE-2020-0625	特权提升	否	否	2	2	N/A
			CVE-2020-0626	特权提升	否	否	2	2	N/A
			CVE-2020-0627	特权提升	否	否	2	2	N/A
			CVE-2020-0628	特权提升	否	否	2	2	N/A
			CVE-2020-0629	特权提升	否	否	2	2	N/A
			CVE-2020-0630	特权提升	否	否	2	2	N/A
			CVE-2020-0631	特权提升	否	否	2	2	N/A
			CVE-2020-0632	特权提升	否	否	2	2	N/A
		Windows 7 for 32-bit Systems Service Pack 1, Windows Server 2008 for 32-bit Systems Service Pack 2	CVE-2020-0634	特权提升	否	否	1	1	N/A
			CVE-2020-0635	特权提升	否	否	2	2	N/A
			CVE-2020-0637	信息泄漏	否	否	4	2	N/A
			CVE-2020-0639	信息泄漏	否	否	2	2	N/A
			CVE-2020-0642	特权提升	否	否	2	2	N/A
			CVE-2020-0643	信息泄漏	否	否	2	2	N/A
4534312	高危		CVE-2020-0615	信息泄漏	否	否	2	2	N/A
			CVE-2020-0608	信息泄漏	否	否	2	2	N/A
			CVE-2020-0620	特权提升	否	否	2	2	N/A
			CVE-2020-0625	特权提升	否	否	2	2	N/A
			CVE-2020-0626	特权提升	否	否	2	2	N/A
			CVE-2020-0627	特权提升	否	否	2	2	N/A
			CVE-2020-0628	特权提升	否	否	2	2	N/A
			CVE-2020-0629	特权提升	否	否	2	2	N/A
			CVE-2020-0630	特权提升	否	否	2	2	N/A
			CVE-2020-0631	特权提升	否	否	2	2	N/A
			CVE-2020-0632	特权提升	否	否	2	2	N/A
			CVE-2020-0634	特权提升	否	否	1	1	N/A
			CVE-2020-0635	特权提升	否	否	2	2	N/A
			CVE-2020-0639	信息泄漏	否	否	2	2	N/A
			CVE-2020-0642	特权提升	否	否	2	2	N/A
			CVE-2020-0643	信息泄漏	否	否	2	2	N/A

4536953	高危	Windows Server 2008 Systems Service Pack 2	ADV990001	深度防御	否	否	0	0	N/A
4536952	高危	Windows 7,Windows Server 2008 R2	ADV990001	深度防御	否	否	0	0	N/A

同时，当月微软发布的软件安全更新补丁共 24 个，选择与 Win7 与 Server 2008 相关的信息列表如下：

KBID	奇安信集团级别	产品	CVE 编号	漏洞的影响	公开披露	已受攻击	最新软件版本	较旧软件版本	拒绝服务
4532959	高危	Security Only Update for .NET Framework 2.0, 3.0 for Windows Server 2008 SP2	CVE-2020-0606	远程执行代码	否	否	2	2	N/A
			CVE-2020-0646	远程执行代码	否	否	2	2	N/A
			CVE-2020-0605	远程执行代码	否	否	2	2	N/A
4532971	高危	Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 SP1 and Windows Server 2008 R2 SP1 and Windows Server 2008 SP2	CVE-2020-0606	远程执行代码	否	否	2	2	N/A
			CVE-2020-0646	远程执行代码	否	否	2	2	N/A
			CVE-2020-0605	远程执行代码	否	否	2	2	N/A

4532964	高危	Security Only Update for .NET Framework 4.5.2 for Windows 7 SP1 and Windows Server 2008 R2 SP1 and Windows Server 2008 SP2	CVE-2020-0606	远程执行代码	否	否	2	2	N/A
			CVE-2020-0646	远程执行代码	否	否	2	2	N/A
			CVE-2020-0605	远程执行代码	否	否	2	2	N/A
4532960	高危	Security Only Update for .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1	CVE-2020-0606	远程执行代码	否	否	2	2	N/A
			CVE-2020-0646	远程执行代码	否	否	2	2	N/A
			CVE-2020-0605	远程执行代码	否	否	2	2	N/A
4532952	高危	Security Only Update for .NET Framework 4.8 for Windows 7 SP1 and Windows Server 2008 R2 SP1	CVE-2020-0606	远程执行代码	否	否	2	2	N/A
			CVE-2020-0646	远程执行代码	否	否	2	2	N/A
			CVE-2020-0605	远程执行代码	否	否	2	2	N/A

注：

1) 上述表格中“软件版本”利用评估等级编号详细说明如下：
   a. **1** - 更有可能被利用
   b. **2** - 不太可能利用
   c. **3** - 不可能利用
   d. **4** - 不受漏洞的影响
2) 拒绝服务（DoS）

a. **永久** 利用此漏洞可能导致操作系统或应用程序永久无响应，直到手动重新启动或意外退出而不自动恢复。同时，任何会导致系统自动重启的漏洞也被视为永久性

3) DoS

a. **临时** 利用此漏洞可能会导致操作系统或应用程序暂时无响应，直到攻击停止，或意外退出但自动恢复。攻击完成后不久，目标将返回正常的功能级别。

b. **不适用（N/A）** 不会遭到 DoS 破坏。

2. 2020 年 1 月 14 日停止服务的 Win7 版本

应注意 Win7 及 Win7 Service Pack 停止服务时间是不一样的（Server 2008 有类似情况），不带 Service Pack 的版本已于 2013 年结束支持，详细列表请查询：
https://support.microsoft.com/zh-cn/lifecycle/search?alpha=Windows%207

此次受影响的版本包括：
Windows 7 Service Pack 1
Windows Embedded Standard 7 Service Pack 1（2020 年 10 月 13 日）

3. Win7 历史上 10 大漏洞

如下以漏洞大多被微软标识为“严重”及以上等级，并曾经引发过业界关注，以下发布时间排序：

1) Win32k 窗口类漏洞 CVE-2010-2744
这是 win7 内核模式驱动程序中出现的漏洞，如果攻击者登录到要攻击的系统中，然后运行经特殊设计的应用程序，就可能拿到本地高级权限。

2) 不安全的库加载漏洞 CVE-2010-3147
这是 Windows 通讯簿（WAB）中出现的漏洞，本地攻击者可以当前工作目录中执行特洛伊木马进而获得特权。

3) Windows MFC 文档标题更新缓冲区溢出漏洞 CVE-2010-3227
这是微软基础类（MFC）库文件 mfc42.dll 中出现的漏洞，远程攻击者可以在某个目录中放置特殊的应用程序并诱骗用户执行，进而可以获得相同的用户权限，并远程执行代码。

4) 驱动程序与 Windows 内核漏洞的不正确交互 CVE-2010-4398
这是 Windows 内核中出现的漏洞。本地攻击者可以在本地登录后运行特殊程序，进而获得权限提升。

5) Windows 传真服务封面编辑器漏洞 CVE-2010-4701
这是 Windows 传真封面编辑器中出现的漏洞。远程攻击者可以构造特制的'.cov'文件并诱骗用户执行，进而执行任意代码。

6) GDI 访问冲突漏洞 CVE-2011-5046
这是 Windows 内核图形设备接口中出现的漏洞，远程攻击者能够执行任意代码，或导致构造特殊数据，实施拒绝服务攻击（DoS）。

7) Win32k 错误的消息处理漏洞 CVE-2013-0008
这是 Win7 和 Server2008 内核模式驱动程序中出现的漏洞，攻击者登录到系统后，可以在本地执行特殊程序，进而获得高等级权限。

8) Win32k.sys 特权提升漏洞 CVE-2014-4113
这是 Win7 内核模式驱动程序 win32k.sys 中出现的漏洞，攻击者登录到系统后，可以在本地执行特殊程序，进而获得高等级权限。

9) Windows OLE 远程执行代码漏洞 CVE-2014-4114
这是 Win7 系统中出现的漏洞,远程攻击者可以在 Office 文档中构建特殊的 OLE 链接对象并诱骗用户执行，进而执行任意代码。该漏洞曾经在 Sandworm APT 攻击中使用过。

10) 目录遍历提权漏洞 CVE-2015-0016
这是 Win7 及 Server2008 系统终端服务组件中出现的漏洞,远程攻击者可以在某个目录中放置特殊的应用程序并诱骗用户执行，进而可以获得相同的用户权限，并远程执行代码。

4. 2020 年 1 月 14 日停止服务的 Server 2008 版本

Server 2008 系列产品较多，一部分产品（包括非 R2，不带 Service Pack 的版本）早于 2011 年就结束了支持，完整的停服列表请查询：
https://support.microsoft.com/zh-cn/lifecycle/search?alpha=windows%20server%202008

此次停服的 Server 2008 版本包括：
Windows Server 2008 R2 Service Pack 1
Windows Server 2008 Service Pack 2

另外，基于 Server 2008 R2 Service Pack 构建的相关产品也于 14 日到期，它们包括：
Windows Storage Server 2008 Basic
Windows Storage Server 2008 Basic 32-bit
Windows Storage Server 2008 Basic Embedded
Windows Storage Server 2008 Basic Embedded 32-bit
Windows Storage Server 2008 Enterprise
Windows Storage Server 2008 Enterprise Embedded
Windows Storage Server 2008 R2
Windows Storage Server 2008 R2 Essentials
Windows Storage Server 2008 Standard

Windows Storage Server 2008 Standard Embedded
Windows Storage Server 2008 Workgroup
Windows Storage Server 2008 Workgroup Embedded
Windows Web Server 2008
Windows Web Server 2008 R2

5. Server 2008 历史上 20 大漏洞

如下以漏洞大多被微软标识为“严重”及以上等级，并曾经引发过业界关注，以下发布时间排序：

1） 远程过程调用漏洞 CVE-2013-3175
远程攻击者可以通过构造格式错误的异步 RPC 请求执行任意代码。

2） Comctl32 整数溢出漏洞 CVE-2013-3195
Windows 通用控件库中的 Comctl32.dll 中出现的漏洞，远程攻击者可以在 ASP.NET Web 应用程序参数中设置特殊值，执行任意代码。

3） Microsoft Schannel 远程执行代码漏洞 CVE-2014-6321
Server 2008 中的 Schannel 出现的漏洞，远程攻击者可以通过特制的数据包执行任意代码。

4） Windows Telnet 服务缓冲区溢出漏洞 CVE-2015-0014
Server 2008 中的 Telnet 服务容易受到缓冲区溢出攻击，远程攻击者可以通过该漏洞，精心制作数据包，并执行任意代码。

5） HTTP.sys 远程执行代码漏洞 CVE-2015-1635
Server 2008 HTTP.sys 文件中出现的漏洞，远程攻击者可以通过特制的 HTTP 请求执行任意代码。

6） Microsoft 通用控件免费使用后漏洞 CVE-2015-1756
Microsoft Common Controls 中出现漏洞，远程攻击者可以通过使用 Internet Explorer 的 F12 开发人员工具功能，诱骗用户访问的特殊的网站，进而执行任意代码。

7） OpenType 字体驱动程序漏洞 CVE-2015-2426
Windows Adobe Type Manager 库中 atmfd.dll 出现的漏洞，远程攻击者可以通过特制的 OpenType 字体执行任意代码。

8） Windows 文件系统特权提升漏洞 CVE-2015-2430
攻击者可以绕过应用程序沙箱保护机制,并通过特制应用程序,执行任意文件系统操作。

9） TrueType 字体解析漏洞 CVE-2015-2464
远程攻击者可以通过特制的 TrueType 字体执行任意代码。

10）远程桌面协议 DLL 植入远程执行代码漏洞 CVE-2015-2473
Server 2008 远程桌面协议（RDP）客户端中出现的漏洞，本地用户可以在当前工作目录中放置特洛伊木马，诱骗高级权限的用户执行，进而获得特权。

11）服务器消息块内存损坏漏洞 CVE-2015-247
经过远程身份验证的用户可以在 Server 2008 服务器消息块（SMB）服务器错误记录操作中放置特制字符串，进而执行任意代码。

12）OpenType 字体解析漏洞 CVE-2015-2506
这是 Server 2008 的 Adobe Type Manager 库文件中出现的漏洞，远程攻击者使用特制的 OpenType 字体，对服务器发起拒绝服务（DoS）攻击。

13）Windows Media Center RCE 漏洞 CVE-2015-2509
这是 Server 2008 中的 Windows Media Center 出现的漏洞，远程攻击者可以使用特制的 Media Center 链接（MCL）文件执行任意代码。

14）图形组件缓冲区溢出漏洞 CVE-2015-2510
这是 Server 2008 中 Adobe Type Manager 库出现的漏洞，远程攻击者可以通过特制的 OpenType 字体执行任意代码。

15）工具栏漏洞 CVE-2015-2515
这是 Server 2008 中存在 After-after-free 漏洞，远程攻击者可以构造特制的工具栏对象，诱骗高权限用户执行，进而可能执行任意代码。

16）Windows Journal RCE 漏洞 CVE-2015-2530
远程攻击者构造特制的.jnt 文件，执行任意代码。

17）Windows Journal 堆溢出漏洞 CVE-2015-6097
这是在 Windows 日记本程序中的漏洞（常见于 Tablet 触屏设备），攻击者可以通过特制的 Journal（.jnt）文件执行任意代码 。

18）图形内存损坏漏洞 CVE-2015-6108
远程攻击者通过构造特制的嵌入式字体执行任意代码。

19）释放漏洞后使用 Windows DNS CVE-2015-6125
这是 Server 2008 DNS 服务中存在 After-after-free 漏洞，远程攻击者通过精心构造的请求执行任意代码。

20）Windows 整数下溢漏洞 CVE-2015-6130
这是 Win8 和 Server 2008 所有版本中都存在的漏洞，远程攻击者可以构造特征的文档或者包含特殊字体的网页，诱骗用户执行，进而远程执行代码。

6. Windows 10 神州网信政府版是政府机构和关键信息基础设施领域用户迁移的最佳选择

入围政采

神州网信政府版已于2017年11月列入软件协议供货入围中央政府采购平台和中直机关采购平台，2019年1月软件协议供货入围中央企业集中采购平台，2019年4月预装Windows 10 神州网信政府版的多家OEM整机入围中央政府采购平台，并获得了用户的一致好评。

安全可控

满足政府及关键信息基础设施领域的安全要求，遥测诊断等外发数据本地管理，无敏感数据出境；集成自研在线升级/更新系统，确保核心组件安全可控。

- 符合政务计算机终端核心配置规范（GB/T-30278）
- 集成国家标准的商密算法SMx（SM2、SM3、SM4）
- 预置国内主要根证书
- 操作系统国内激活（多种方式）
- 操作系统国内更新（多种方式）
- 数据外发控制
- 默认多重安全防护

技术先进

新一代操作系统平台，提供最新操作系统功能特性，确保与用户的信息化架构同步更新，提升用户使用满意度，更好地服务于用户的信息化平台。

- 主流设备驱动全自动更新
- 多设备全平台一致性一体化操作系统
- 支持多工作区（虚拟桌面）方便用户在不同应用桌面自由切换
- 全新的用户操作控制中心
- 原生触屏及平板模式支持

优化体验

- 保持用户良好的开始菜单体验
- 精简与政企用户业务无关的应用
- 简化用户操作界面，提升工作效率
- 支持多任务预览视图

国内生态

操作系统周边生态建设是政企用户广泛采纳的基础因素，基于最新操作系统技术构建，神州网信目前已与国内各领域主流供应商建立了合作关系，适配新的软硬件产品，建设全方位的生态体系。

合作伙伴主要涉及：安全软件、基础软件、系统软件、行业应用、整机厂商、硬件厂商等。

7. 奇安信天擎是一体化安全防护体系

奇安信天擎是冬奥组会官方网络安全服务和杀毒软件赞助商，也是微软和神州网信的长期合作伙伴。2019 年 IDC 报告显示，奇安信位列中国终端安全软件市场占有率第一。奇安信终端安全防护体系从威胁防御、终端管理、安全运营三个维度出发，为企业构造全新的立体终端安全架构。

1) **防御维度**：通过威胁防御、系统加固、安检合规、威胁分析、数据保护、资产管理六个方面，构建企业终端安全自运营的安全体系。
2) **管理维度**，通过统一管理、安全可视、协同联动三个方面，构建企业终端安全自运营的管理体系。
3) **运营维度**，通过自主建设、自动编排、自适应防御三个方面，构建企业终端安全的智能运营体系。

奇安信天擎通过该体系实现终端的全面统一管理，以及威胁入侵过程中的检测响应能力，通过对安全策略进行持续改进和验证，确保在内外部环境不断变化的背景下，始终保持企业终端的安全闭环。

奇安信天擎是个产品族，至少包括如下这些核心组件，更多详细资料请查询：

- **终端安全管理系统**，https://www.qianxin.com/product/detail/pid/49
- **终端安全管理系统（信创版）**，https://www.qianxin.com/product/detail/pid/50
- **终端安全响应系统（EDR）**，https://www.qianxin.com/product/detail/pid/52
- **终端安全准入系统**，https://www.qianxin.com/product/detail/pid/53
- **终端安全运营**，https://www.qianxin.com/product/detail/pid/54

  IoT 接入控制系统，https://www.qianxin.com/product/detail/pid/58

8. 奇安信云锁服务器安全管理系统是主机安全产品

奇安信服务器安全管理系统是中国用户总量领先的主机安全产品，在国际上率先达到 Gartner 定义的 cwpp（云工作负载保护平台）标准、EDR(终端检测与响应)+EPP(Endpoint Protection Platform)标准，兼容多种虚拟化架构和操作系统，可以高效支撑现代混合数据中心架构下的主机安全需求。

奇安信服务器安全管理系统基于服务器端轻量级 agent，安全加固服务器操作系统及应用，奇安信服务器安全管理系统 waf 探针、rasp 探针、内核加固探针能有效检测与抵御已知、未知恶意代码和黑客攻击；同时奇安信服务器安全管理系统融合资产管理、微隔离、攻击溯源、自动化运维、基线检查等强大功能，帮助用户高效安全运维服务器。