企业主机安全

最新动态

文档版本 01

发布日期 2022-01-20

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 最新动态

本文介绍了企业主机安全（Host Security Service，HSS）各特性版本的功能发布和对应的文档动态，欢迎体验。

2021 年 12 月

序号	功能名称	功能描述	阶段	相关文档
1	HSS新增远程代码执行漏洞的检测能力	新增Apache Log4j2的远程代码执行漏洞（CVE-2021-44228、CVE-2021-45046）的检测能力。	商用	服务公告 开启网页防篡改

2021 年 10 月

序号	功能名称	功能描述	阶段	相关文档
1	手动检测软件信息	实时检测主机中的风险和异常操作，在每日凌晨将对主机执行全面扫描，此外，您也可以使用手动检测功能全面检测主机中关键的配置信息。	商用	手动检测软件信息

2021 年 5 月

序号	功能名称	功能描述	阶段	相关文档
1	HSS新增漏洞检测能力	新增HTTP 协议堆栈远程执行代码漏洞、Hyper-V 远程执行代码漏洞、OLE 自动化远程执行代码漏洞、脚本引擎内存损坏漏洞4个严重漏洞的检测能力。	商用	查看漏洞详情

2020 年 12 月

序号	功能名称	功能描述	阶段	相关文档
1	Linux勒索病毒防护	• 创建Linux防护策略时，若开启诱饵防护，HSS将会在关联服务器上预置诱饵文件。若发现未知勒索病毒加密诱饵文件的行为，立即告警。 • 创建Linux防护策略完成后，智能学习策略通过机器学习引擎学习关联服务器上的可信进程修改文件的行为，对绕过诱饵文件的勒索病毒进行告警。	商用	Linux勒索病毒防护
2	升级配额规格	若您当前的防护配额的版本无法满足您的业务需求，您可以根据需要将企业主机安全服务的版本升级为“企业版”、“旗舰版”或者“网页防篡改版”。	商用	升级配额规格
3	批量解绑配额	您可以通过防护配额页面，批量解绑配额。 解绑配额后，HSS会关闭主机防护，无法检测主机存在的潜在风险，请谨慎操作。	商用	解绑配额

2020 年 9 月

序号	功能名称	功能描述	阶段	相关文档
1	所有项目	在“所有项目”中，对您拥有的所有主机进行批量安全配置，可避免您到每个企业项目中对主机进行重复配置。 若对其中某一个企业项目中的安全配置有差异化需求，您可以到具体的企业项目中进行单独配置。 在某个企业项目中的差异化配置是独立的，对其他企业项目不产生影响。	商用	管理所有项目

2020 年 6 月

序号	功能名称	功能描述	阶段	相关文档
1	勒索病毒防护	勒索病毒防护功能可有效监控您云主机上存储的重要文件，防止未经过认证或授权的进程文件对监控文件的加密或修改操作，保障您的主机不被勒索病毒侵害。	商用	勒索病毒防护
2	程序运行认证	程序运行认证功能支持将重点防御的主机加入到白名单策略中，通过检测白名单中指定的应用程序区分“可信”、“不可信”和“未知”，防止未经白名单授权的程序运行。 可避免您的主机受到不可信或恶意程序的侵害，还能防止不必要的资源浪费、保证您的资源被合理利用。	商用	程序运行认证
3	一键漏洞修复、验证	HSS检测Linux漏洞、Windows漏洞和Web-CMS漏洞，并为Linux漏洞和Windows漏洞提供一键漏洞修复、验证功能。	商用	一键漏洞修复

2020 年 5 月

序号	功能名称	功能描述	阶段	相关文档
1	文件完整性管理	文件完整性管理功能检查操作系统、应用程序软件和其他组件的文件，确定它们是否发生了可能遭受攻击的更改，同时，能够帮助用户通过PCI-DSS等安全认证。 文件完整性管理功能是使用对比的方法来确定当前文件状态是否不同于上次扫描该文件时的状态，利用这种对比来确定文件是否发生了有效或可疑的修改。	商用	文件完整性管理
2	批量导入/导出告警白名单	您可以通过批量导入/导出告警白名单避免大量告警误报的发生，提升安全事件告警质量。	商用	告警白名单

2020 年 4 月

序号	功能名称	功能描述	阶段	相关文档
1	旗舰版主机安全重磅推出	旗舰版主机安全，全端统管，主动防御、智能检测、安全运营，全方位防护保障主机安全，轻松应对安全威胁，彻底阻断入侵行为，轻松高效管理运营平台，是下一代主机安全的新标杆！ 新增功能： • 威胁检测类型从7大类增加至13大类，增加反弹Shell、异常Shell、高危命令执行、自启动检测、提权操作和Rootkit程序六大类威胁检测能力 • 新增程序运行认证功能 • 新增关键文件校验功能 • 新增策略管理功能 • 新增告警白名单功能 • 新增服务器组功能	商用	旗舰版

2019 年 10 月

序号	功能名称	功能描述	阶段	相关文档
1	支持鲲鹏云主机	为用户提供主机管理、风险预防、入侵检测、高级防御、安全运营、网页防篡改功能，全面识别并管理鲲鹏主机中的信息资产，实时监测您的鲲鹏云主机中的风险并阻止非法入侵行为，全方位保障您的鲲鹏云主机安全。	商用	安全配置

2019 年 9 月

序号	功能名称	功能描述	阶段	相关文档
1	动态网页防篡改	提供tomcat应用运行时自我保护，能够检测针对数据库等动态数据的篡改行为。	商用	开启动态网页防篡改

2018 年 8 月

发布时间	功能名称	功能描述	阶段	相关文档
2018.08.30	企业主机安全网页防篡改版	网页防篡改可实时监控网站目录，并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入恐怖威胁、色情等内容，是政府、院校及企业等组织必备的安全服务。	商用	网页防篡改
2018.08.16	企业主机安全上线	企业主机安全是提升主机整体安全性的服务，为用户提供资产管理、漏洞管理、入侵检测、基线检查等功能，降低主机被入侵的风险。	商用	什么是企业主机安全服务?