主机安全

动态与公告

腾讯云

文档目录

动态与公告
产品动态

最近更新时间：2024-07-22 18:04:11

本文将为您展示主机安全产品的历史发布记录。

2024年07月

动态名称	动态描述	发布时间	相关文档
新增反弹 Shell 白名单	新增反弹 Shell 正则加白功能，支持通过正则表达式配置命令特征白名单，提高检出率。	2024-07-16	-
新增反弹 Shell 自动拦截重保模式	针对反弹 Shell 的自动拦截功能新增重保模式，综合多个引擎检测结果，针对中、高置信度的风险进行自动拦截，适用于重保防护。	2024-07-16	-
新增文件查杀自动拦截重保模式	针对文件查杀的自动拦截功能新增重保模式，综合多个引擎检测结果，针对中、高置信度的风险进行自动拦截，适用于重保防护。	2024-07-16	-
新增恶意请求自动拦截重保模式	针对恶意请求的自动拦截功能新增重保模式，综合多个引擎检测结果，针对中、高置信度的风险进行自动拦截，适用于重保防护。	2024-07-16	-
新增高危命令自动拦截重保模式	针对高危命令的自动拦截功能新增重保模式，综合多个引擎检测结果，针对中、高置信度的风险进行自动拦截，适用于重保防护。	2024-07-16	-

2024年06月

动态名称	动态描述	发布时间	相关文档
新增内网反弹 Shell 检测	新增内网反弹 Shell 检测功能，用户可自定义开启或关闭内网告警检测开关，也可配置告警列表是否展示内网告警数据。	2024-06-26	-
新增恶意请求自动拦截	新增恶意请求自动拦截功能，开启后，支持自动拦截检测出的系统黑域名和黑IP，	2024-06-26	-

	终止进程对黑域名/黑 IP 的访问。		
新增高危命令自动拦截	新增高危命令自动拦截功能，开启后，支持自动拦截检测出的系统高危命令，查杀命中规则的进程。	2024-06-26	-

2024年03月

动态名称	动态描述	发布时间	相关文档
新增日志类型	新增网络五元组日志、文件监控日志、登录流水日志，用户可在日志分析中自定义选择是否要存储网络五元组日志、文件监控日志、登录流水日志等，便于在排查风险时进行关联取证和深度风险排查。	2024-03-28	日志分析
日志存储告警	机器人通知支持日志分析存储告警，当日志存储量达到用户配置值时触发日志存储告警，提醒用户及时扩容，避免关键日志数据丢失。	2024-03-28	-

2024年01月

动态名称	动态描述	发布时间	相关文档
基础版支持密码破解阻断	基础版支持按情报规则和登录规则进行密码破解阻断判定，自动阻断仅支持对威胁情报中的黑 IP 进行阻断。	2024-01-25	密码破解
混合云接入 AK 同步资产	可同步阿里云 ECS 机器数据（不论何种操作系统均可拉取），但安装 Agent 目前还是需要手动操作。	2024-01-25	主机列表
停售专业版-按量计费	主机安全购买页正式下线专业版-按量计费选项，存量已选择自动加购按量计费的客户仍可持续扩容/新购。	2024-01-25	功能介绍与版本比较

2023年10月

动态名称	动态描述	发布时间	相关文档
新增日志类型	新增主机安全客户端上报日志类型，支持存储主机原始日志、DNS 日志、进程快照日志；默认存储 DNS 日志和进程快照日志；主机原始日志包含如：系统认证和授权信息、系统安全信息、系统消息、系统审计信息等内容。	2023-10-27	日志分析

2023年09月

动态名称	动态描述	发布时间	相关文档
客户端支持系统更新	主机安全客户端安装覆盖更多版本的Linux操作系统，如：TencentOS Server、Tencent tlinux、OpenCloudOS、AlmaLinux、OpenSUSE、Rocky、Red Hat 6及以上版本、Aliyun Linux、Amazon Linux。	2023-09-27	主机列表
启动服务支持自启动项检测	支持获取启动服务当前的启动状态，检测该启动服务是否为自启动项，便于用户观察和统计自启动项的变更情况。	2023-09-27	资产指纹
机器人通知支持飞书平台Webhook	支持将告警消息通过飞书平台的 Webhook 地址推送到飞书消息群中。	2023-09-27	-

2023年08月

动态名称	动态描述	发布时间	相关文档
支持机器人通知	支持企微、钉钉、飞书、自定义 Webhook 告警，告警内容可选择文本格式、JSON 格式，支持自定义透传字段，用户可对透传字段进行判定，进一步做告警降噪处理。 （注：灰度中，如有实时告警需求请 联系我们 获取）	2023-08-30	-

2023年06月

动态名称	动态描述	发布时间	相关文档
网络攻击改版	网络攻击支持在主机端对恶意攻击流量进行感知，实时监测恶意攻击行为，覆盖云上热点漏洞，支持南北向、东西向的攻击流量检测。支持统计攻击数据分布、攻击来源 TOP5等图表，完善网络攻击列表字段和详情，支持标记已处理、开启漏洞防御、加入白名单、忽略、删除记录，支持选择尝试攻击、攻击成功的事件类型进行告警。	2023-06-20	网络攻击
新增存储设置和告警	日志分析服务支持配置存储内容；支持配置存储时长，每月支持2次修改，超出存储时长的日志将自动清除；每月最后一天的存储情况将展示在存储记录中，便于用户了解每月存储变化情	2023-06-02	日志分析

	况；支持存储告警，当已使用存储量达到一定数值将触发告警。		
新增日志存储内容	存储内容支持存储主机列表、资产指纹变更流水日志。	2023-06-02	主机列表 资产指纹
新增“必修漏洞”标签	针对威胁等级严重、高危，全网攻击热度高的漏洞标记“必修漏洞”标签，便于用户重点关注和处理。	2023-06-02	漏洞管理
漏洞防御能力增强	漏洞防御新支持如下漏洞： • Dubbo 漏洞防御 • Confluence 远程代码执行漏洞（CVE-2019-3396） • Confluence Sharelinks SSRFÅ • Jenkins 远程代码执行漏洞（CVE-2019-1003000） • CloudBees Jenkins GitHub Plugin SSRF pcmgr-105907 • CloudBees Jenkins 安全漏洞 pcmgr-182169	2023-06-02	漏洞管理
授权管理优化	授权隔离期缩短：主机安全普惠版/专业版/旗舰版安全防护授权的隔离期时长，由30天隔离期缩短为7天。	2023-06-02	授权管理

2023年04月

动态名称	动态描述	发布时间	相关文档
新增事件调查	• 主机安全旗舰版主机（Linux 系统）支持高危命令、恶意文件、恶意请求、暴力破解、本地提权、反弹 Shell、异常登录功能部分情况的告警和溯源，通过进程树综合关联多类告警，从入侵链路的角度达到事件调查的效果。 • 事件调查精准自动分析和关联相关入侵告警信息，图形化展示黑客入侵链路，并引导用户处理相关安全告警，帮助安全运维减轻工作量，提升运维效率。	2023-04-30	主机列表
新增"读取文件"监控	核心文件监控规则配置中，可选择监控“读取文件”、“修改文件”行为，当对文件的操作行为命中了规则将触发告警，支持在控制台对告警标记已处理、加入白名单、忽略或删除记录，可添加核心文件监控规则来实现对文件的读/写实时监控、自动告警通知。	2023-04-30	核心文件监控

新增授权支持关联项目和标签	主机安全防护授权新支持关联项目和标签，以满足客户希望通过项目、标签进行分类或分账的使用场景。	2023-04-30	授权管理
优化基线策略	存在多基线策略的情况下，关闭某一策略会自动清除该策略以往的检测结果，从而避免对整体基线通过率产生影响。	2023-04-30	基线管理

2023年02月

动态名称	动态描述	发布时间	相关文档
新增混合云代理接入	新支持公网代理接入：混合云场景中安装主机安全客户端，用户可根据自身服务器情况选择单台 nginx 代理、VIP 高可用集群（可通过 VIP + Keepalived 或负载均衡实现）。 非腾讯云服务器支持获取公网 IP：混合云场景中，主机安全客户端新支持对阿里云、亚马逊云服务器公网 IP 的获取。	2023-02-23	主机列表
新增进程树启动时间	文件查杀-恶意文件、高危命令、本地提权、反弹 Shell、核心文件监控的进程树均新增进程启动时间字段。	2023-02-16	• 文件查杀 • 高危命令 • 本地提权 • 反弹 Shell • 核心文件监控
漏洞防御能力增强	漏洞防御新支持如下漏洞： • LOG4J_CVE-2021-45105 • LOG4J_CVE-2021-44832 • Tomcat WebSocket CVE-2020-13935 • Tomcat AJP文件包含漏洞（CVE-2020-1938）	2023-02-09	漏洞管理

2023年01月

动态名称	动态描述	发布时间	相关文档

优化主机列表	• 客户端离线时间展示：在主机列表中，针对客户端已离线的情况，支持查看客户端最后离线时间。 • 主机详情展示标签：在主机详情页中支持展示标签（腾讯云标签、主机安全标签），支持对标签进行编辑，并在导出列表中新增腾讯云标签和主机安全标签字段。	2023-01-26	主机列表

2022年12月

动态名称	动态描述	发布时间	相关文档
优化主机列表	• 新增资产清理：腾讯云服务器销毁后将会自动被清理；非腾讯云服务器，支持设置离线一定时间后自动清理的规则。 • 优化主机展示形式：控制台中主机展示形式改为主机名称/实例 ID、IP 地址（公网和内网），并支持多关键字模糊筛选。	2022-12-29	主机列表
漏洞防御能力增强	漏洞防御新支持如下漏洞： • Nexus Repository Manager 3 弱口令(计划任务 RCE) • Spring messaging Spel（CVE-2018-1270） • Nexus Repository Manager 3 远程命令执行漏洞（CVE-2020-10204） • Spring Data Commons Spel 注入（CVE-2018-1273） • Nexus Repository Manager 3 远程命令执行漏洞（CVE-2019-7238） • Spring 框架反射型文件下载漏洞 (CVE-2020-5421) • Jackson 漏洞防御 • XStream 漏洞防御	2022-12-29	漏洞管理
授权一键删除	在授权管理中，支持一键删除所有过期/作废的授权。	2022-12-29	授权管理
自动升级防护开关拆分	原自动升级防护拆分为自动绑定和自动加购两个开关。 • 自动绑定开关开启时当检测到您账号下存在基础版主机时，将自动与您账号下的可用授权进行绑定。 • 自动加购开关开启时若可用授权不足，将自动扩容或新购您指定版本的授权（会产生一定费用）再自动绑定。	2022-12-29	授权管理
新增异常进程检测功能	针对 Linux 系统的云服务器内存进行异常进程扫描，以解决加壳/加密等场景下静态二进制特征无法检测的问题，可对异常进程进行查杀等处理操作。	2022-12-12	文件查杀

2022年11月

动态名称	动态描述	发布时间	相关文档
支持启发式引擎	在查杀设置页面的实时监控中，支持启发式引擎开启/关闭，开启则采用严格的模式实时扫描系统 Webshell。	2022-11-24	文件查杀
新增云立体防护模块	支持试用三道防线产品，即 WAF/CFW/CWP&TCSS。	2022-11-24	-
优化导出功能	主机列表、漏洞管理支持腾讯云标签分列展示，与 CVM 对齐，便于客户在表格中做表头筛选，并支持导出。	2022-11-24	主机列表
新增客户端离线/卸载API接口	支持带 appid 查询客户端离线（服务器内网 IP、实例 ID、客户端离线时间）和客户端卸载（服务器内网 IP、实例 ID、客户端卸载时间、卸载命令调用链）	2022-11-17	获取客户端异常事件
支持内网日志投递	支持通过内网投递，只需选择消息队列实例、输入用户名密码、连通性测试通过即可进行内网投递。	2022-11-07	日志分析

2022年10月

动态名称	动态描述	发布时间	相关文档
漏洞防御能力增强	漏洞防御新支持如下漏洞： • Apache Druid 远程代码执行漏洞（CVE-2021-25646） • Apache Commons Text StringLookup 远程代码执行漏洞 (CVE-2022-42889) • Fastjson 反序列化任意代码执行漏洞 • JBoss readonly Java 反序列化漏洞（CVE-2017-12149） • JBoss Application Server JBossMQ JMS 反序列化漏洞 • JBoss /invoker/JMXInvokerServlet 反序列化漏洞（CVE-2015-7501） • JBoss EJBInvokerServlet Marshalled Object 代码执行漏洞	2022-10-27	漏洞管理
异常登录优化	新增待处理说明、解决白名单 IP 和地域设置冲突。	2022-10-27	异常登录

小程序接口数据优化	安全评分、各项风险数值、风险趋势、实时动态与主机安全控制台对齐。	2022-10-27	-

2022年09月

动态名称	动态描述	发布时间	相关文档
新增自动拦截功能	恶意请求、高危命令支持设置黑名单拦截策略，监测到主机对恶意 DNS 进行外联请求、主机存在高危命令时进行自动拦截操作，增强安全事件事中处理能力。	2022-09-29	恶意请求 高危命令
新增日志投递 Ckafka	支持将入侵检测、漏洞管理、基线管理、高级防御、客户端离线/卸载等安全事件日志投递至 Ckafka。便于用户统一管理服务器日志数据。	2022-09-29	日志分析
支持 TAT 单机自动安装客户端	服务器满足4个条件（属于 CVM 或 Lighthouse、开机状态、处于 VPC 网络、已安装 TAT）支持在主机安全中自动安装客户端。减少用户手动安装的繁琐操作。	2022-09-29	主机列表
漏洞防御能力增强	漏洞防御新支持如下漏洞： • Atlassian Confluence OGNL 表达式注入命令执行漏洞（CVE-2021-26084） • Apache Shiro默认Key远程命令执行漏洞（CVE-2016-4437） • CVE-2019-0193 Apache Solr 远程命令执行漏洞 • CVE-2019-17558 Apache Solr Velocity 模板注入漏洞 • CVE-2016-3088 Apache ActiveMQ fileserver 文件上传漏洞 • CVE-2018-1000861 Jenkins-远程命令执行漏洞 • Fastjson 反序列化任意代码执行漏洞 • Apache Druid 远程代码执行漏洞（CVE-2021-25646）	2022-09-29	漏洞管理

2022年08月

动态名称	动态描述	发布时间	相关文档

基线优化	• 基线提供白名单规则体系，帮助用户按规则批量忽略不适配的基线规则。 • 基线提供弱口令自定义能力（旗舰版主机适用），允许用增加自己的弱口令规则。	2022-08-25	基线管理
支持新建文件白名单规则	用户可通过文件名、文件 MD5、文件目录等多种方法，批量忽略上报不准确的恶意文件信息。	2022-08-25	文件查杀
支持日志投递功能	日志分析服务现已支持日志投递功能。	2022-08-16	日志分析
漏洞防御上线	旗舰版主机现可开启漏洞防御功能。	2022-08-08	漏洞管理

2022年07月

动态名称	动态描述	发布时间	相关文档
新增漏洞防御	支持自动在云服务器上生效虚拟补丁，有效拦截黑客攻击行为，为客户修复漏洞争取时间。	2022-07-28	漏洞管理

2022年06月

动态名称	动态描述	发布时间	相关文档
新增 Java 内存马	支持自动检测主机上 JavaWeb 服务进程，注入检测探针插件到服务进程中，实时监控黑客通过漏洞、Shell 等注入的 Java 内存马。 支持自定义配置插件开关状态，查看插件注入/运行状态及错误日志。	2022-06-30	Java 内存马
新增主机安全普惠版	主机安全与轻量应用服务器产品形态融合，合作推出普惠版，为用户提供便捷实惠的主机安全能力。普惠版提供主机安全四大基础功能：异常登录、密码破解、文件查杀、应急漏洞；在实例详情页中即可闭环使用主机安全基础功能，降低用户认知成本。	2022-06-30	-
优化安全播报订阅	安全播报支持消息订阅，触达用户，提升客户对于安全情报的获得感。	2022-06-30	-

产品公告
关于《主机安全服务等级协议》的更新通知

最近更新时间：2024-05-13 16:51:51

尊敬的腾讯云用户，您好！

为了给您带来更持续稳定的服务体验，我们已于2024年05月13日更新《主机安全服务等级协议》，将主机安全的服务可用性从99.9%提高至99.95%。

> **说明：**
> 2024年05月13日起，适用新服务可用性比例；2024年05月13日前，仍按原服务可用性比例执行。

感谢您对主机安全的信赖与支持！

关于主机安全日志分析服务购买规格及价格调整的通知

最近更新时间：2024-04-19 14:45:41

尊敬的腾讯云用户，您好！
主机安全近期将新增支持存储网络五元组、文件监控、登录流水等客户端上报日志，预期日志存储量将大幅增加，为更好地满足您的业务需求，自**2024年05月09日起**，我们将对日志分析服务购买规格及价格进行调整。

调整内容

1. 存储容量购买步长：由50GB扩大为1TB。
2. 价格：由1元/GB/月下调至0.5元/GB/月。

调整影响

调整后，对存量已购日志分析的客户有如下影响：
1. 若订单未过期，续费、扩容的费用将按下调后的价格计费（仍可按50GB步长来扩容）。
2. 若订单已过期，重新新购将按下调后的价格计费，存储容量购买步长为1TB。

感谢您对腾讯云主机安全的信赖与支持，若在使用过程中有任何问题可以 提交工单 反馈给我们，我们将尽快为您核实处理！

关于主机安全停止支持防护 Windows server 2003服务器的通知

最近更新时间：2024-03-28 17:22:11

尊敬的腾讯云用户，您好！

由于市面上使用 Windows Server 2003操作系统的服务器数量较少，主机安全已于北京时间**2024年03月28日起**停止支持防护操作系统版本为 Windows Server 2003的服务器，可支持的操作系统请参见 快速入门，给您带来不便，敬请谅解。

感谢您对主机安全的支持与关注！

关于《主机安全服务等级协议》与《主机安全服务条款》的更新通知

最近更新时间：2024-03-08 11:30:01

尊敬的腾讯云用户，您好！
为了给您提供更好的产品使用保障，主机安全计划将于**2024年03月15日**对《主机安全服务等级协议》与《主机安全服务条款》的内容进行更新。

- 更新《主机安全服务等级协议》
  付费版本补充旗舰版，专业版和旗舰版服务承诺业务可用性提升至99.9%，以更好地满足您的需求并提供更可靠的服务。

- 更新《主机安全服务条款》
  针对主机安全客户端离线导致主机被勒索的场景，补充使用规则和责任限制条款，以明确我们在此类情况下的责任范围。

相关内容将于2024年03月15日更新并正式生效，请您关注更新内容并在使用服务前审慎阅读，特别请您关注关于限制、免责条款或者其他涉及您重大权益的条款。

感谢您对主机安全的信赖与支持，在此期间有任何问题，您可通过 在线客服 咨询，我们将竭诚为您服务！