Cyber Security Products Guide

优秀网络安全产品指南

2021.02

赛可达实验室

前言

本版指南覆盖 16 类 34 个产品，产品都是近三年“赛可达优秀产品奖（SKD AWARDS）”获奖产品，经过了国际知名第三方网络安全服务机构——赛可达实验室专业测试团队的严格测试。赛可达实验室依据国内外最新产品标准和发展趋势，在接近真实应用场景中，对产品表现做了全面测试，验证了获奖产品的功能和性能。所列产品彰显出了它们在网络安全行业各自细分领域的国际先进水准。

《优秀网络安全产品指南》和“年度赛可达优秀产品奖（SKD AWARDS）”旨在助力行业用户了解和选择最适合的产品和解决方案，使网络更安全；同时，助力安全企业技术创新，打造世界级产品，提升品牌知名度，增强国内外市场竞争力。

“年度赛可达优秀产品奖（SKD AWARDS）”自 2013 年成功举办至今，得到了国内外网络安全界的认可，被誉为“网络安全产品的奥斯卡”，已成为衡量网络安全产品水平的重要指标之一。

赛可达实验室
skd labs

赛可达实验室

赛可达实验室（SKD Labs）是国际知名第三方网络安全服务提供商，也是中国合格评定国家认可委员会 CNAS 认可实验室以及国际 ISO/IEC 17025 认证实验室。实验室拥有世界领先的网络安全检测技术、数年丰富的国际测评经验和专业的测试团队，秉承“公正、中立、科学、严谨”的服务理念，致力为政企用户和安全企业提供权威的第三方网络安全服务。服务范围包含软硬件产品安全测评认证、网络安全有效性检测评估、APP 安全合规检测认证、产品入围选型测试、渗透测试、项目验收测试、通用软件测评、代码安全审计等。

软硬件产品安全测评范围包括防火墙、主机防护、反病毒、APP、UTM、移动安全、APT、终端安全、云安全、反垃圾邮件、网关、流量管理和监控、负载均衡、OTA，以及 VPN、IPS、IDS、WAF、上网行为管理、漏洞检测和扫描设备、路由器、交换机、智能设备等网络信息安全软硬件产品。

目 录

APT

御界高级威胁检测系统 ---------- 1

OTA

百度安全 OTA ---------- 2

PC 浏览器

360 安全浏览器 ---------- 3

PC 终端安全

电脑管家小团队版 ---------- 4

腾讯电脑管家 ---------- 5

测试仪表

安全与应用性能测试解决方案 C200 ---------- 6

思博伦 CF20 应用与安全测试解决方案 ---------- 7

防毒墙

蓝盾防毒墙 ---------- 8

瑞星防毒墙（RSW） ---------- 9

工控网络安全

天地和兴工控安全审计平台 HX-IMAP ---------- 10

威努特工控漏洞挖掘平台 Vhunter IVM ---------- 11

漏洞检测

漏洞之眼 (BUGEYES) ---------- 12

企业终端安全

安天智甲终端检测与响应系统 ---- 13
辰信领创防病毒系统 ---- 14
美创诺亚防勒索系统 ---- 15
奇安信天擎终端安全管理系统 (EDR) ---- 16
瑞星 ESM（下一代网络版） ---- 17
深信服终端检测响应平台 EDR ---- 18
亚信安全高级威胁终端检测及响应系统 ---- 19
亚信安全端点安全管理系统 ESM ---- 20

杀毒引擎

SAVE 安全智能检测引擎 ---- 21
奇安信 OWL 反病毒引擎 (QOWL) ---- 22

渗透测试平台

悬镜灵脉 IAST 灰盒安全测试平台 ---- 23

数据安全

美创数据脱敏系统 ---- 24
天空卫士内部威胁管理平台 ---- 25

威胁情报

暗网空间测绘雷达系统 ---- 26

移动终端安全

腾讯手机管家 ---- 27

云安全

京东云 Network Fast 1 应用交付控制器 ---- 28
京东云 DDoS 防护与流量调度系统 ---- 29
京东云态势感知与安全运营中心 ---- 30
京东云应用安全网关 ---- 31

主机安全

腾讯云主机安全 ---------- 32

网宿智能入侵检测引擎 ---------- 33

悬镜云卫士 ---------- 34

产品名称：御界高级威胁检测系统

产品网址：https://s.tencent.com/product/gjwxjc/index.html

腾讯御界
Tencent Security

产品介绍

御界高级威胁检测系统（下简称御界），是基于腾讯安全的安全能力、依托腾讯在云和端的海量数据，研发出的独特的恶意威胁检测系统。通过镜像方式采集企业网络边界流量，对流量进行解析，还原文件，通过入侵规则、威胁情报匹配，沙箱文件分析等多重技术手段识别威胁。同时，运用大数据技术关联多项信息，对攻击源、目的进行大数据分析识别。此外，系统将对流量日志，告警报文进行存储，并提供高效的大数据交互式查询功能，方便事后对安全事件的追踪溯源。针对1G、3G、10G及以上等不同的网络流量环境，御界提供不同的部署模式。

适用领域

适用于政府、能源、运营商、金融、教育、医疗等大、中、小型客户的网络威胁检测、APT检测、流量威胁溯源分析。

公司简介

Tencent 腾讯

公司名称：腾讯科技有限公司

公司简介：腾讯，1998年11月诞生于中国深圳，是一家以互联网为基础的科技与文化公司。我们的使命是“通过互联网服务提升人类生活品质”。腾讯秉承着 “一切以用户价值为依归”的经营理念，为亿万网民提供优质的互联网综合服务。腾讯的战略目标是“连接一切”，我们长期致力于社交平台与数字内容两大核心业务：一方面实现人与人、服务及设备的智慧连接；另一方面为数以亿计的用户提供优质数字内容产品及相关服务。腾讯希望成为各行各业的数字化助手，助力数字中国建设。腾讯的愿景是成为“最受尊敬的互联网企业”。我们始终坚守“科技向善”的初心，运用科技手段助力公益事业发展，并将社会责任融入每一个产品。

网址：https://www.tencent.com/　　电话：0755-86399799　　邮箱：es@tencent.com

OTA

产品名称：百度安全OTA

产品网址：https://ota.baidu.com/

产品介绍

百度安全OTA是由百度安全推出，主打安全高效的智能IoT设备OTA升级解决方案，集成百度安全多项专利技术，提供云端下发平台、web端管理平台及设备端SDK（适配Android、Linux、RTOS等主流系统），旨在为智能设备提供低成本、便捷接入、功能完善的固件及设备应用升级服务。

适用领域

1. 智能家居设备：智能音箱、智能冰箱、智能空调、智能电视、智能网关、扫地机器人、安防摄像头…
2. 智能穿戴设备：运动手表、儿童可通话手表、智能血压计、随身音乐播放器…
3. 互联网汽车整车及配件：Tbox、动力控制系统、汽车娱乐系统、行车记录仪…
4. 各垂直领域有屏设备：智能售卖机、共享充电宝分发设备、大屏可交互导航机、手持扫码设备、各式购票取票设备…

公司简介

百度安全
有AI更安全

公司名称：百度安全

公司简介：百度安全是百度公司旗下，以AI为核心、大数据为基础打造的领先安全品牌，是百度在互联网安全18年最佳实践的总结与提炼。业务由AI安全、移动安全、云安全、数据安全、业务安全五大矩阵构成，全面覆盖百度各种复杂业务场景，同时向个人用户和商业伙伴输出领先的安全产品与行业一体化解决方案。

百度安全以技术开源、专利共享、标准驱动为理念，联合互联网公司、安全厂商、终端制造商、高校及科研机构， 推动AI时代的安全生态建设，让全行业享受更安全的AI所来带来的变革。

网址：https://anquan.baidu.com/　**电话：**400-805-4999　**邮箱：**wenhuiyuan@baidu.com

PC浏览器

产品名称：360安全浏览器

产品网址：https://browser.360.cn/se/

360安全浏览器
360 SECURITY BROWSER

产品介绍

360安全浏览器是互联网上安全好用的新一代浏览器，拥有国内领先的恶意网址库，采用云查杀引擎，可自动拦截挂马、欺诈、网银仿冒等恶意网址。独创的“隔离模式”，让用户在访问木马网站时也不会感染。无痕浏览，能够更大限度保护用户的上网隐私。360安全浏览器体积小巧、速度快、极少崩溃，并拥有翻译、截图、鼠标手势、广告过滤等几十种实用功能，已成为广大网民上网的优先选择。

适用领域

所有人群及所有网页浏览场景。

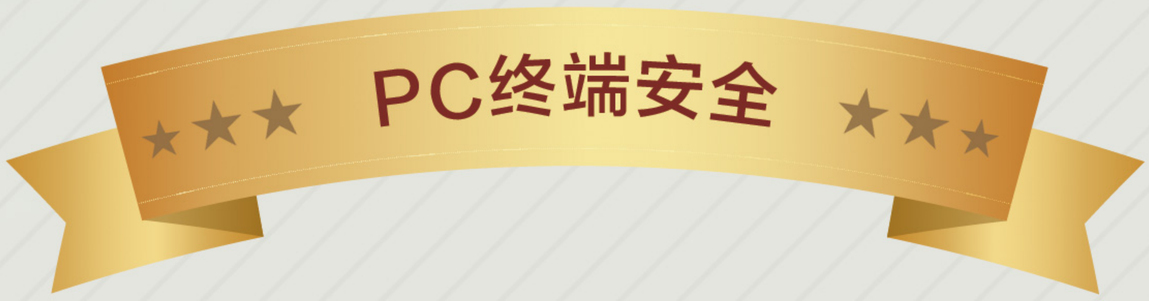
公司简介

360 www.360.cn

公司名称：北京奇元科技有限公司

公司简介：作为中国领先的互联网络安全企业，汇聚了国内规模领先的高水平安全技术团队，积累了接近万件原创技术和核心技术的专利，并在此基础上开发出拥有数亿用户的360安全卫士、360手机卫士等安全产品，同时为上百万家国家机关和企事业单位提供包括安全咨询、安全运维、安全培训等全方位安全服务。

网址：https://www.360.cn/　　电话：15010316652　　邮箱：zhaoshengnan@360.cn



产品名称：电脑管家小团队版

产品网址：https://team.qq.com/site/index.html

产品介绍

电脑管家小团队版是腾讯电脑管家团队倾情打造的运维管理工具，旨在为中小微企业提供团队内设备管理、运行状态查看、定时关机等运维服务，降低企业成本，提高效率。

适用领域

中小微企业的IT管理员。

公司简介

公司名称：腾讯科技

公司简介：腾讯以技术丰富互联网用户的生活。通过通信及社交平台微信和 QQ 促进用户联系，并助其连接数字内容和生活服务，尽在弹指间。通过高效广告平台，协助品牌和市场营销者触达数以亿计的中国消费者。通过金融科技及企业服务，促进合作伙伴业务发展，助力实现数字化升级。我们大力投资于人才队伍和推动科技创新，积极参与互联网行业协同发展。腾讯于 1998 年11月在中国深圳成立，2004 年6月在香港联合交易所主板上市。

网址：https://www.tencent.com/zh-cn/index.html 电话：0755-86399799 邮箱：es@tencent.com

PC终端安全

产品名称：腾讯电脑管家

产品网址：https://guanjia.qq.com

产品介绍

腾讯电脑管家是腾讯出品的国际领先的互联网安全产品、安全服务提供者，能够有效预防和解决电脑上存在的安全管理问题。拥有实时防护、病毒木马云查杀，帐号保护，漏洞修复及清理加速等全方位的安全管理功能。依托管家云查杀引擎、腾讯TAV杀毒引擎和系统修复引擎，管家产品多次在AV-C、赛可达等全球权威评测中摘得桂冠！同时，电脑管家13版本推出权限雷达功能，第一次将安卓系统的权限管理用于PC，能够管理电脑上软件行为，屏蔽软件弹窗、阻止软件推装等，还用户纯净的办公和游戏环境。电脑管家安全防护能力和管理能力已达到国际一流水平，时刻守护数亿用户。

适用领域

全部用户。

公司简介

公司名称：腾讯

公司简介：腾讯以技术丰富互联网用户的生活。通过通信及社交平台微信和 QQ 促进用户联系，并助其连接数字内容和生活服务，尽在弹指间。通过高效广告平台，协助品牌和市场营销者触达数以亿计的中国消费者。通过金融科技及企业服务，促进合作伙伴业务发展，助力实现数字化升级。我们大力投资于人才队伍和推动科技创新，积极参与互联网行业协同发展。腾讯于 1998 年11月在中国深圳成立，2004 年6月在香港联合交易所主板上市。

网址：https://www.tencent.com/zh-cn/index.html **电话：**0755-86399799 **邮箱：**es@tencent.com

测试仪表

产品名称：安全与应用性能测试解决方案 C200

产品网址：https://www.spirent.com/-/media/datasheets/security/ds-spirent-c200-appliance.pdf?la=en&hash=5FD97B906A111C56F6EB321D9FAB1DE4D9B24A47

产品介绍

适用于CyberFlood和Avalanche的C200设备仅凭借轻薄小巧的1U机箱尺寸便可提供业界最高的性能和容量，并支持10G、25G、40G、50G和100G多种速率。用户可以利用它对网络基础设施、Web应用和媒体服务的安全和性能极限进行评估，确保客户获得的服务质量（QoS）和体验质量（QoE）。C200与CyberFlood和Avalanche评估解决方案完全兼容，能够帮助您实现具备最丰富多样性的应用层测试。C200可用于应用性能测试、Web应用测试、高性能HTTPS/TLS测试、安全测试/验证、攻击和恶意软件评估、先进DDoS仿真、VPN/IPsec性能、包含13000余种应用场景的应用识别测试、先进视频应用测试、移动网络防火墙测试以及大规模回放UDP/TCP流量等。

适用领域

安全设备厂商、网络安全测评机构、网络安全政府部门、企业网络安全部门、关注网络安全领域的高等院校和科研单位。

公司简介

公司名称：思博伦通信

公司简介：思博伦通信（LSE：SPT）是在测试、保障、分析与安全、服务开发商和供应商以及及企业网络领域拥有深厚专业知识和几十年丰富经验的全球领导者。致力于明晰越来越复杂的技术和商业挑战。思博伦的客户为实现优越性能许诺，思博伦为客户兑现承诺给予保障。

思博伦提供先进的性能分析与服务保证解决方案，从有线到无线再到卫星通信，拥有全面的测试解决方案，这些解决方案能够帮助客户顺利的开发和部署下一代网络技术。

网址：www.spirent.com　**电话：**010-85182539　**邮箱：**Bo.qu@spirent.com

测试仪表

产品名称：思博伦 CF20 应用与安全测试解决方案

产品网址：https://www.spirent.com/products/cyberflood

产品介绍

思博伦CyberFlood产品家族的CF20可作为1G、10G、40G和100G接口的高级测试选项。CF20可测试网络基础设施和Web应用基础设施的有效性和性能，对您的安全态势、服务质量（QoS）和体验质量（QoE）进行验证。CF20充分利用了Cyber-Flood的强大能力，将多种测试功能合并到小型独立设备中，为您提供更高的使用便利性。

- 利用真实的攻击和入侵验证安全有效性；
- 测试DDoS消减服务和下一代防火墙；
- 创建极端的HTTPS流量负载，对加密容量和性能进行验证；
- 利用不断更新的数据库来生成各类应用负载流量，其中包含超过10,000种应用场景和应用流，能够对应用ID策略和性能执行全面验证；
- 利用当日和最新恶意软件样例执行测试；
- 回放大规模的定制流量；
- 先进的模糊攻击测试可创建出数以百万计的测试场景，迅速、高效地发现未知的漏洞。

适用领域

安全设备厂商、网络安全测评机构、网络安全政府部门、企业网络安全部门、关注网络安全领域的高等院校和科研单位。

公司简介

公司名称：思博伦通信

公司简介：思博伦通信（LSE：SPT）是在测试、保障、分析与安全、服务开发商和供应商以及及企业网络领域拥有深厚专业知识和几十年丰富经验的全球领导者。致力于明晰越来越复杂的技术和商业挑战。思博伦的客户为实现优越性能许诺，思博伦为客户兑现承诺给予保障。思博伦提供先进的性能分析与服务保证解决方案，从有线到无线再到卫星通信，拥有全面的测试解决方案，这些解决方案能够帮助客户顺利的开发和部署下一代网络技术。

网址：www.spirent.com 、www.spirent.cn　**电话：**010-85182539　**邮箱：**Bo.qu@spirent.com

防毒墙

产品名称：蓝盾防毒墙（BDAI-AVW）

产品网址：http://www.bluedon.com/security_detail-01-10.html

产品介绍

蓝盾防毒墙在传统病毒特征查杀引擎基础上，引入基于机器学习威胁检测的人工智能病毒查杀引擎，从而同时具备对已知病毒和未知病毒查杀，弥补了传统引擎对未知病毒查杀盲区，为网络防病毒提供可靠保障。

产品特色：1.高性能基础平台：采用多核并发架构，数据包无需排队；一体化安全引擎，避免重复解析数据包；零拷贝技术，内存共享避免拷贝动作；2.全面安全防护：企业级防火墙；网络流量深度解析；多维度访问控制；抗 DDOS 攻击；连接数控制；会话管理；3.AI病毒检测技术：采用千万级样本训练模型；不断训练更新模型；检测速度在毫秒级；能有效识别病毒木马变种；准确率达到 99%；4. 云端沙箱仿真环境：配置云端沙箱仿真环境，兼容多种文件格式；独有的防沙箱逃逸技术；强大的专家分析团队对沙箱运行结果进行分析。

适用领域

适用于金融、军队、政府等各行业。

公司简介

蓝盾 BLUEDON 智慧安全领导者 蓝盾股份:300297

公司名称：蓝盾信息安全技术股份有限公司

公司简介：蓝盾股份是中国信息安全行业的领军企业，公司成立于1999年，并于2012年3月15日在深交所创业板上市。公司构建了以安全产品为基础，覆盖安全方案、安全服务、安全运营的完整业务生态，为各大行业客户提供一站式的信息安全整体解决方案。同时，公司也瞄准了信息安全外延不断扩大的趋势，通过“自主研发+投资并购”双轮驱动的方式，持续推进“大安全”产业发展战略，并以“技术升级”、“空间拓展”、“IT层级突破”三个维度为主线进行布局，构建了完整的“大安全”产业生态版图。

网址：www.bluedon.com　电话：020-85526663　邮箱：zsm@chinabluedon.cn

防毒墙

产品名称：瑞星防毒墙（RSW）

产品网址：http://ep.rising.com.cn/bianjie/2017-08-10/18952.html

产品介绍

瑞星防毒墙（RSW）是一款部署于内部网络与外部网络之间的具备高性能和高稳定性的网络安全系统，它的目的就是将内部网络和Internet网络进行一个逻辑的隔离，以保障内部网络数据的安全。瑞星防毒墙集多种安全技术于一身，包括网络防火墙、防病毒、抗DoS、防恶意站点、VPN、Web内容过滤、流量控制以及日志报表等安全管理功能，用户无需安装任何附件软件，便可以极大程度的提高企业网络的安全性。

瑞星防毒墙支持多种网口工作模式，适用于各种复杂的网络拓扑环境，通过实施安全策略可以在网络环境中的内外网之间建立一道功能强大的防火墙体系，使得在病毒进入网络前便可以得到阻拦。

作为一个应用在网络边缘的安全产品，瑞星防毒墙能够与现有网络安全产品无缝结合，实现了与瑞星网络安全威胁感知系统、瑞星预警系统、瑞星网络版杀毒软件、瑞星ESM终端安全管理软件的联动机制，能够为用户提供从终端到网关、从点到面的整体安全解决方案。

适用领域

政府、央企、军工、军队、公检法司、电力、能源、金融、电信、教育、企事业单位等。

公司简介

RISING 瑞星

公司名称：北京瑞星网安技术股份有限公司

公司简介：北京瑞星网安技术股份有限公司创立于1991年，一直专注于信息安全领域，坚持自主研发，拥有完整的自主知识产权，帮助政府、企业及个人有效应对信息安全威胁，主要业务包括企业及个人两大部分。瑞星企业级信息安全整体解决方案分四大类，包括终端安全解决方案、云安全解决方案、网关安全解决方案、安全教育解决方案。

网址：http://www.rising.com.cn/　　**电话：**010-82678866　　**邮箱：**liuhw@rising.com.cn

工控网络安全

产品名称：天地和兴工控安全审计平台HX-IMAP

产品网址：http://www.tdhxkj.com/index.php/shenjileichan-pin/2019/04-15/176.html

产品介绍

天地和兴工控安全审计平台HX-IMAP是天地和兴公司面向电力、石油石化、轨道交通、钢铁冶金、智能制造等工业行业自主研发的安全审计产品。工控安全审计平台HX-IMAP能够实时检测针对工业协议的网络攻击、用户误操作、用户违规操作、非法设备接入以及蠕虫、病毒等恶意软件的传播并实时报警，同时详实记录一切网络通信行为，包括指令级的工业控制协议通信记录，为工业控制系统的安全事故调查提供坚实的基础。

适用领域

适用电力、石油石化、轨道交通、钢铁冶金、智能制造、烟草、水利等工业行业。

公司简介

天地和兴 Tiandihexing

公司名称：北京天地和兴科技有限公司

公司简介：北京天地和兴科技有限公司成立于2007年，是国内较早从事工控信息安全的安全厂商。覆盖电力行业、石油石化、轨道交通、智能制造、钢铁冶金和军工等多个关键基础设施领域。始终秉承“打造可信控制环境、助力网络强国战略”的企业使命，为用户提供安全检查、风险评估、安全培训、安全测评等全方位的专业服务。总部设在北京，先后在武汉、青岛、珠海、杭州、呼和浩特、乌鲁木齐、成都成立分子公司及办事处负责产品研发、咨询服务和市场营销等方面工作。形成了以全生命周期工控系统信息安全整体解决方案为核心的客户服务体系。同时公司持续加大对新技术、新产品的研发力度，依托浙江大学“工控系统安全联合研究中心”及华北电力大学“电力工业信息安全联合实验室”等科研机构不断深入对工控漏洞、人工智能安全、大数据态势分析等方向的技术研究。

网址：www.tdhxkj.com　**电话：**010-82896289　**邮箱：**tdhx@tdhxkj.com

工控网络安全

产品名称：威努特工控漏洞挖掘平台（VHunter IVM）

产品网址：http://www.winicssec.com/product/l124.html

产品介绍

威努特工控漏洞挖掘平台（VHunter IVM）是由威努特自主研发用于发现工控设备未知漏洞、验证其安全状况的黑盒测试产品，产品采用智能Fuzzing技术，对工控设备（PLC、RTU 等）、工控系统（DCS、SCADA等）进行未知漏洞挖掘、安全性和健壮性测试，深度挖掘工控设备或系统的各类已知、未知漏洞，产品可自动生成ISASecure标准的测试报告，清晰定位问题并提供测试报文便于问题回溯，能显著的提升工业控制系统的安全性。

全球六个荣获ISASecure CRT Test Tools安全认证证书的产品之一；全面覆盖工业互联网协议；热插拔式多接口类型业务板卡；高精度彩色液晶屏显示；软硬件结合自动化循环分段故障定位。

适用领域

■ 为监管机构提供技术支撑：通过工控漏洞挖掘平台对工控网络中的PCL、DCS、RTU等工控设备进行健壮性和安全性测试，挖掘未知漏洞，有效补充行业监管机构在漏洞发现方面的能力。

■ 为工控安全审查提供专业工具支撑：工控漏洞挖掘为国产自主知识产权的专业化工具，其测试能力得到国际权威认可，能很好的支撑工控安全审查体系的建立。

■ 帮助工业控制系统厂商争取更多的市场空间：工控漏洞挖掘能自动化发现设备潜在漏洞，显著提高工控设备安全测试效率、降低安全测试成本，帮助工控系统厂商赢取更多的市场占有率。

公司简介

威努特 WINICSSEC

公司名称：北京威努特技术有限公司

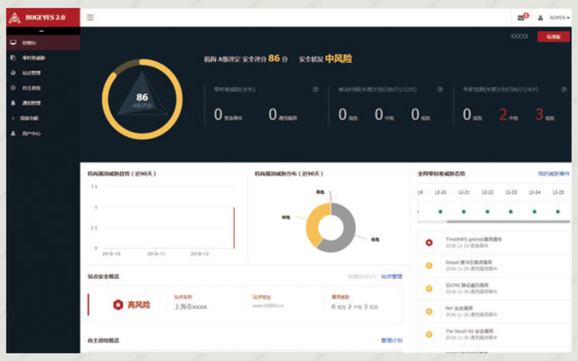
公司简介：北京威努特技术有限公司（以下简称“威努特”）， 是国内工控网络安全领军企业、全球六家荣获国际自动化协会安全合规学会ISASecure CRT Tool认证企业之一和亚太地区唯一国际自动化学会（ISA）全球网络安全联盟(GCA)创始成员。威努特作为国家高新技术企业，以创新的“白环境”整体解决方案为核心，自主研发了5大类30款全系列网络安全专用产品，拥有64项发明专利、64项软件著作权、70项原创漏洞证明等核心知识产权。积极牵头和参与工控网络安全领域国家、行业标准制定。迄今已成功为电力、轨道交通、石油石化、军工、烟草、市政、智能制造、冶金等国家重要行业1000多家工业企业提供了全面有效的安全保障。

网址：winicssec.com　　电话：010-62977816　　邮箱：support@winicssec.com

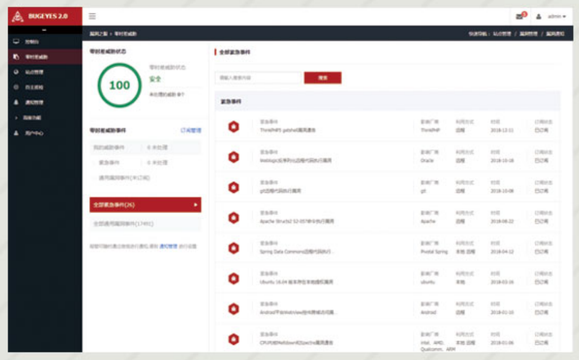
漏洞检测

产品名称：漏洞之眼（BUGEYES）

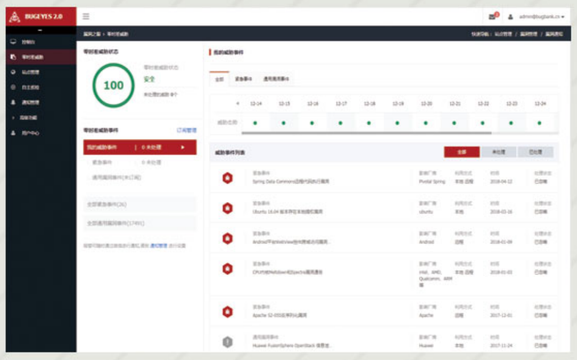
产品网址：www.bugeyes.cn



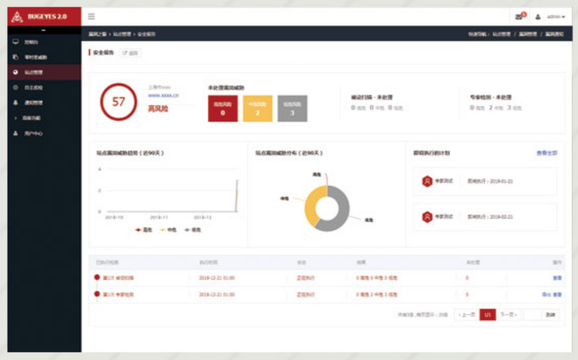
首页



紧急事件



零时差威胁



站点报告

产品介绍

漏洞之眼针对机构网站提供上万名专家联合诊断服务，通过模拟黑客入侵过程，从黑客视角对机构进行安全测试，深度发掘各类高危漏洞。系统动态调用多个检测系统，在最短时间内覆盖多项安全检测，更高效的完成安全检测工作。系统每日搜集全网安全事件与威胁情报，第一时间将最新0day以报告的形式推送给用户。漏洞之眼与专属安全工程师根据用户漏洞修复情况与检测排期计划定期对已发现漏洞进行回归测试，同时借助漏洞生命周期管理为漏洞的修复状态进行标注，通过多种途径定期提醒用户存在尚未修复的漏洞。

适用领域

具有互联网应用系统的机构和企业单位。

公司简介

漏洞银行 BUGBANK

公司名称：上海谋乐网络科技有限公司

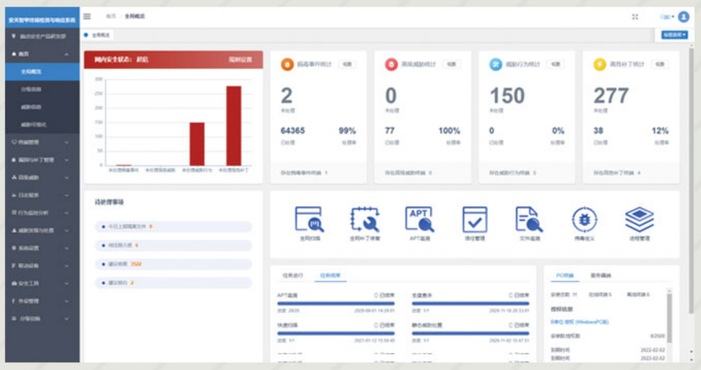
公司简介：上海谋乐网络科技有限公司，成立于2012年，是由一支充满激情与创造力，并有着丰富安全及互联网经验的团队所成立。公司是上海创新性互联网安全企业，现主要服务于金融、证券、互联网、电商、政府等行业。首创了入侵追踪系统（ITS概念），公司目前主要面向企业的信息安全，公司主要业务内容为网站安全评估、渗透性测试、安全咨询、等保整改咨询、信息安全建设解决方案、安全运维，安全培训与应急响应。公司主要产品为一云流量防御系统、漏洞之眼漏洞威胁平台和CADC城域主动防御中心。

网址：bugbank.cn　　电话：021-67628100　　邮箱：mia@bugbank.cn

企业终端安全

产品名称：安天智甲终端检测与响应系统

产品网址：https://www.antiy.cn/



产品介绍

安天智甲终端检测与响应系统主要面向服务器、办公机等主机，提供安全数据采集、威胁深度分析、威胁/可疑事件告警、威胁事件响应等服务。产品主要功能包括：1.数据采集：支持对主机的资产信息、配置信息、文件信息、进程信息、网络信息、外设使用等进行细粒度采集，并支持形成可定制化的采集方案；2.资产管理：支持展示资产相信信息，并支持进行策略配置，任务下发等；3.告警展示：支持对上报的数据进行深度分析，并形成丰富的事件告警；4.追踪溯源：支持展示威胁程序的全部行为动作，以及关联的可疑程序，对病毒的攻击过程进行展示；5.事件响应：支持对各类安全事件进行不同方式的处理，包括文件删除、进程停止、环境恢复、端口封堵、补丁修复等。

性能：客户端程序大小≤20MB，CPU占用≤5%，内存占用≤50MB；单终端网络单次通信流量≤4KB。

适用领域

主要目标行业政府、电力、能源、军工、部队、金融、教育、制造业等，支持防护的终端类型包括：服务器、虚拟化终端、办公机、专用设备等。

公司简介

安天

公司名称：北京安天网络安全技术有限公司

公司简介：安天致力于全面提升客户的网络安全防御能力，有效应对安全威胁。通过多年自主研发积累，安天形成了威胁检测引擎、高级威胁对抗、大规模威胁自动化分析等方面的技术领先优势。构筑由铸岳、智甲、镇关、探海、捕风、追影、拓痕、智信组成的产品方阵，可以为客户构建资产运维、端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置等安全基础能力。安天通过为客户建设态势感知平台体系，形成网络安全运行的神经中枢，提升客户统一安全运维能力，并通过快捷精准的威胁情报持续完成客户赋能。安天的产品和解决方案保障客户从办公内网、私有云、混合云到工业生产网络的全面安全，保障客户关键数据资产安全和业务运行连续性。

网址：https://www.antiy.cn/　电话：400-840-9234　邮箱：support@antiy.cn

企业终端安全

产品名称：辰信领创防病毒系统

产品网址：www.v-secure.cn

产品介绍

辰信领创防病毒系统（以下简称“辰信领创防病毒”）以尖端的反病毒技术、高效的查杀性能、易用的操作界面，诠释下一代人工智能防病毒软件。对引擎技术的不断研究，使辰信领创防病毒引擎拥有了高检出、低误报、小体积的优秀品质，并结合私有云查杀的优势，使得辰信领创防病毒更加符合国内企业用户的安全习惯。辰信领创防病毒遵循闭环概念，能够从全网角度设立多重筛查机制，达到超细粒度的文件检测和病毒清除，层层过滤确保不会放过任何可疑文件。

- 集中管控：辰信领创防病毒集北信源、启明星辰多年终端安全管理经验，通过景云级联中控平台，提供可伸缩的跨平台病毒防护，集中管控各级各类泛终端，满足企业级用户对防病毒软件统一管理的需求。
- 智慧云查：辰信领创防病毒是面向企业级用户的私有云防病毒解决方案，集成国际领先的私有云安全系统，可为用户按需定制云知识库，智能自运营云端病毒特征，使用户在拥有公有云的病毒查杀能力的同时，又通过私有化的方式彻底杜绝数据泄露。
- 强效性能：辰信领创防病毒一直以更轻、更快、更准为首要研究方向，在降低用户终端资源消耗同时，结合人工智能和大数据技术，能使病毒查杀更迅速、更精准。能够有效防御最流行的病毒木马、恶意网站、黑客入侵和 0day、APT 等未知威胁。

适用领域

政府、企事业单位。

公司简介

辰信领创 V-secure Technology

公司名称：北京辰信领创信息技术有限公司

公司简介：北京辰信领创信息技术有限公司（以下简称“辰信领创”）成立于2016年7月，是一家以人工智能、物联网终端安全为目标的创新型公司。通过数据挖掘、机器学习等人工智能技术，实现对物联网海量数据及本地网络行为的自动化挖掘，并与云端关联分析，实现从物联终端到云端完整的、全方位的、立体化的智能安全防护体系。在强化传统终端安全防护能力的同时，基于大数据分析与机器学习技术实现恶意入侵行为的检测，智能识别物联网网络攻击，同步提升对移动终端、物联网终端、社交网络前端、可穿戴设备等智能终端领域安全能力的覆盖。辰信领创将秉承“让用户放心使用终端”的宗旨，始终致力于给用户提供一流的技术、产品和服务。

网址：www.v-secure.cn　　电话：010—57265747　　邮箱：heixue@v-secure.cn

企业终端安全

产品名称：美创诺亚防勒索系统

产品网址：http://www.mchz.com.cn/cn/product/Noah-FLS/

产品介绍

美创诺亚防勒索系统采用主动防护的模式，利用底层驱动技术，监控所有进程的写操作，对文件的“写”操作判断，对于非法写操作进行阻断。通过控制文件的“写”权限，从而对勒索病毒的写操作进行控制，就算被植入勒索病毒，勒索病毒也无法对文件进行加密，就能保证该办公电脑或者服务器彻底免除勒索病毒的困扰。通过白名单机制监控所有进程，精准识别文件的操作行为，确保只有被允许的合法操作才能被执行，避免勒索病毒对文件加密和修改。即使业务系统未及时安装补丁，可防止漏洞被利用进行勒索加密。

适用领域

办公电脑防勒索；服务器防勒索；分支机构防勒索；哑终端防勒索。

公司简介

公司名称：杭州美创科技有限公司

公司简介：杭州美创科技有限公司（以下简称“美创科技”）成立于2005年，公司以“聚焦数据安全、释放数据价值”为己任，从数据角度出发，围绕数据安全、数据治理、容灾备份、运行安全等方面进行数据安全防护和数据资产管理。美创科技总部位于杭州，分支服务机构遍布全国。作为国家高新技术企业、省级企业研究院，公司十分注重科技创新、持续产品研发。数据库防水坝、数据脱敏、数据库防火墙、数据库审计、全业务容灾、运维一体机等产品均获得了权威测评机构认证与市场认可。目前公司产品和服务被广泛地应用于医疗、政府、社保、金融、港口物流、电力能源等众多行业。

网址：www.mchz.com.cn　**电话：**400-811-3777　**邮箱：**marketing@mchz.com.cn

企业终端安全

产品名称：奇安信天擎终端安全管理系统

产品网址：https://www.qianxin.com/product/detail/pid/52

产品介绍

奇安信天擎终端安全管理系统，是面向政企单位推出的一体化终端安全产品解决方案。该产品集防病毒、终端安全管控、终端准入、终端审计、外设管控、EDR等功能于一体，兼容不同操作系统和计算平台，帮助客户实现平台一体化、功能一体化、数据一体化的终端安全立体防护。

终端检测与响应（EDR）是“天擎”的重要组成部分，其通过威胁情报、攻防对抗、机器学习等方式，从主机、网络、用户、文件等维度来评估企业网络中存在的未知风险，以行为引擎为核心，利用威胁情报，缩短威胁从发现到处置的时间，有效降低业务损失，增加可见性，提升整体安全能力。EDR的主要功能包括：1.终端大数据采集；2.主动式威胁检测；3.终端威胁追踪；4.威胁应急响应。

适用领域

终端检测与响应（EDR）可广泛运用于政企客户办公终端及业务服务器，通过持续的检测与响应，为用户提供终端安全的积极防御能力，其典型适用场景包括：1. 基于威胁线索进行安全事件分析调查；2.基于已确定事件定位威胁源及受影响范围；3. 利用高级检索规则常态化、实战化进行主动安全检测；4. 统一下发威胁处置策略。

公司简介

奇安信 新一代网络安全领军者

公司名称：奇安信科技集团股份有限公司

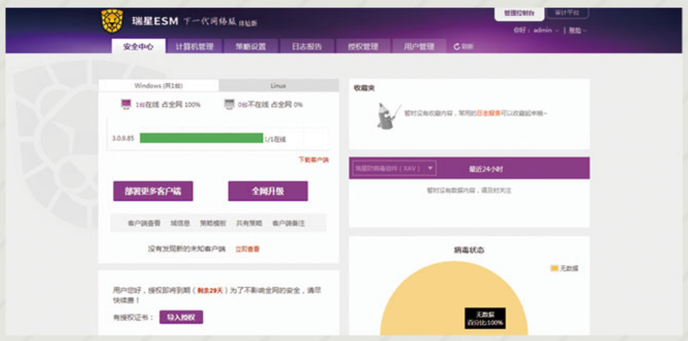
公司简介：奇安信科技集团股份有限公司（股票代码688561）成立于2014年，专注于网络空间安全市场，为向政府、企业用户提供新一代企业级网络安全产品和服务。凭借持续的研发创新和以实战攻防为核心的安全能力，已发展成为国内领先的基于大数据、人工智能和安全运营技术的网络安全供应商。同时，奇安信是2022年冬奥会和冬残奥会网络安全服务与杀毒软件的官方赞助商；此外，公司已在印度尼西亚、新加坡、加拿大、中国香港等国家和地区开展网络安全业务。

网址：https://www.qianxin.com/　　电话：4009-303-120　　邮箱：kefu@qianxin.com

★★★企业级终端安全★★★

产品名称：瑞星ESM（下一代网络版）

产品网址：http://ep.rising.com.cn/zhongduan/18998.html



产品介绍

瑞星ESM（下一代网络版）软件是北京瑞星网安技术股份有限公司开发的新一代企业级终端安全管理系统软件。产品集主机防病毒、防火墙、漏洞扫描、资产管理、行为审计功能于一体，为用户提供了一整套完整的终端安全解决方案。

在统一化的管理平台上，支持物理机、虚拟机，Windows、Linux一体化统一管控，并适配了大量国产平台Linux、专用机等，适用于政府、企业、金融、军队、医疗、教育、制造业等各类企事业单位，是各行业推行网络及终端安全的解决方案的首选。

瑞星ESM采用B/S、C/S混合架构，由中心（包括：数据中心、管理中心、业务中心、扩展中心）、终端、远程控制台几部分共同组成，分布式体系结构分工明确，支持大型网络环境，管理维护方便，同时可满足将来其它安全功能的扩充。

适用领域

政府、央企、军工、军队、公检法司、电力、能源、金融、电信、教育、企事业单位等。

公司简介

RISING 瑞星

公司名称：北京瑞星网安技术股份有限公司

公司简介：北京瑞星网安技术股份有限公司创立于1991年，一直专注于网络安全领域，以优质的产品和专业的服务，向政府、企业及个人提供基于终端安全、云安全、网关安全、安全教育等核心技术的整体解决方案。

瑞星旗下所有产品均为自主研发，拥有100%自主知识产权。瑞星作为国内唯一一家拥有完整自主知识产权的网络安全整体解决方案提供商，在国内设有监控中心、研发中心和病毒响应中心等，为所有用户提供最完整、领先的安全服务。

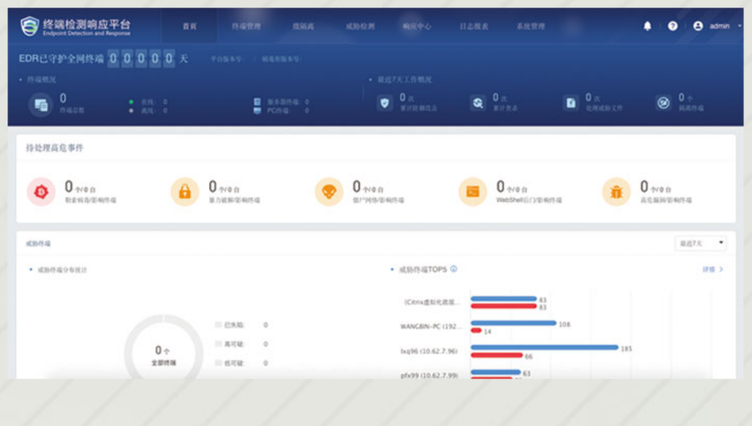
瑞星公司是具有认证资质的高新技术企业，依托十余年坚持不懈的产品技术创新和项目经验积累，在国内网络安全市场中赢得了良好的声誉及口碑，并已经完成多次政府信息安全保障工作，为大型会议、活动提供强有力的专业化信息安全服务。

网址：http://www.rising.com.cn/　　电话：010-82678866　　邮箱：zhangyi@rising.com.cn

企业终端安全

产品名称：深信服终端检测响应平台EDR

产品网址：http://www.sangfor.com.cn/product/net-safe-mobile-security-edr.html?utm_outerpage=www.baidu.com/link



产品介绍

EDR终端检测响应平台是深信服围绕终端安全而推出的一款产品。通过围绕终端资产安全生命周期，通过预防、防御、检测、响应赋予终端更为细致的隔离策略、更为精准的查杀能力、更为持续的检测能力、更为快速的处置能力。在应对高级威胁的同时，通过云网端联动协同、威胁情报共享、多层级响应机制，帮助用户快速处置终端安全问题，构建轻量级、智能化、响应快的下一代终端安全系统。目前客户群体包括国家电网，CNCERT，京东方，国家卫健委，国家气象局等等行业TOP客户，已有效保护终端超过200W。

适用领域

政府，企业，教育，医疗，能源等等各领域用户。

适用于全类型资产的闭环安全防护，包括桌面云，传统PC，笔记本，私有云，服务器，私有云，公有云全适配，与底层虚拟化解耦，适配全部虚拟化底层平台。

公司简介

SANGFOR 深信服科技

公司名称：深信服科技股份有限公司

公司简介：深信服科技股份有限公司是一家专注于企业级安全、云计算及基础架构的产品和服务供应商，拥有智安全、云计算和新IT三大业务品牌，致力于承载各行业用户数字化转型过程中的基石性工作，从而让用户的IT更简单、更安全、更有价值。目前，深信服在全球设有50余个分支机构，公司先后被评为国家级高新技术企业、下一代互联网信息安全技术国家地方联合工程实验室、广东省智能云计算工程技术研究中心等。深信服坚持以持续创新的理念为用户打造省心便捷的产品，获得了市场广泛认可。目前，近10万家用户正在使用深信服的产品。根据IDC数据，深信服硬件VPN、SSL VPN、上网行为管理、广域网优化等多款产品，多年来保持中国市场占有率第一。

网址：http://www.sangfor.com.cn　电话：400-806-0282/0755-86627888　邮箱：thy@sangfor.com.cn

企业终端安全

产品名称：亚信安全高级威胁终端检测及响应系统CTDI

产品网址：https://www.asiainfo-sec.com/contents/2919/12315.html

产品介绍

亚信安全高级威胁终端检测及响应系统采用EDR技术通过对操作系统行为高清记录和长期存储，对操作系统、应用软件和账号资产进行动态发现，根据威胁行为规则IOA和外部特征库IOC来对漏洞攻击和无文件攻击等高级威胁进行关联分析及检测，通过绘制进程事件树实现攻击可视化，对受害主机进行远程遏制和修复。

适用领域

提供给用户进行终端高级威胁检测和溯源。

公司简介

亚信安全

公司名称：亚信安全科技股份有限公司

公司简介：亚信安全是既“懂网”又“懂云”的网络安全公司。承继亚信20余年精准敏锐的电信服务市场洞察和数字化服务经验，以及10余年云安全的核心技术积淀，亚信安全持续引航网络安全的发展和创新。

亚信安全以安全数字世界为愿景，以护航产业互联网为使命，在云安全、身份安全、终端安全、安全管理、数据安全、高级威胁治理和威胁情报等7大领域拥有核心技术。亚信安全是国家身份认证体系和身份安全的核心技术力量，守护亿级用户的每一次网络接入和认证。依托平台级网络安全解决方案与服务，亚信安全不断助推5G时代的网安技术创新。

网址：www.asiainfo-sec.com　　电话：800-820 8876　　邮箱：lu.di@asiainfo-sec.com

企业终端安全

产品名称：亚信安全终端安全管理系统ESM

产品网址：https://www.asiainfo-sec.com/contents/2919/12313.html

产品介绍

亚信安全端点安全管理系统 ESM 是针对安全威胁升级变化实现统一管理的新一代终端安全解决方案。为用户提供了包括防病毒、EDR、虚拟补丁、资产管理、外设管控等丰富的安全防护功能，并对传统威胁和高级威胁提供集检测、遏制、调查和修复的威胁全生命周期的管理体系。端点安全管理系统 ESM 具备了包含恶意软件检测引擎、攻击行为检测引擎、机器学习检测引擎和威胁情报数据湖的“三擎一湖”技术，集成了威胁情报、攻防对抗、机器学习等多种能力，可为用户提供更加安全可靠的计算环境。

亚信安全端点安全管理系统 ESM 广泛地适配信创架构（x86、ARM 和 MIPS）以及主流国产操作系统平台（麒麟、统信、中科方德等），已经与麒麟、统信、长城和浪潮等信创软硬件厂商取得了互认，为用户的信创端点安全替换提供平滑升级过渡。

适用领域

致力于建设终端安全一体化或提升端点安全防护能力的企业用户。

公司简介

亚信安全

公司名称：亚信安全科技股份有限公司

公司简介：亚信安全是既“懂网”又“懂云”的网络安全公司。承继亚信20余年精准敏锐的电信服务市场洞察和数字化服务经验，以及10余年云安全的核心技术积淀，亚信安全持续引航网络安全的发展和创新。

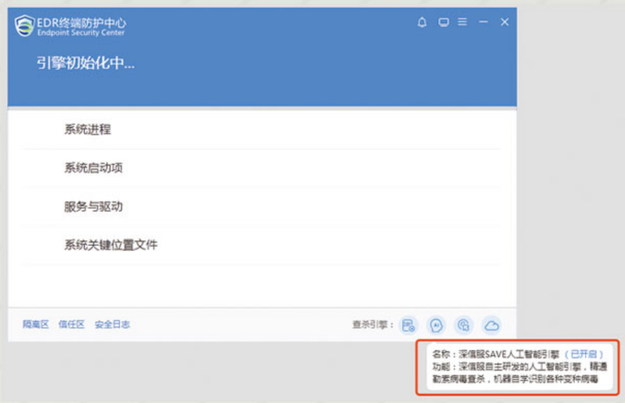
亚信安全以安全数字世界为愿景，以护航产业互联网为使命，在云安全、身份安全、终端安全、安全管理、数据安全、高级威胁治理和威胁情报等7大领域拥有核心技术。亚信安全是国家身份认证体系和身份安全的核心技术力量，守护亿级用户的每一次网络接入和认证。依托平台级网络安全解决方案与服务，亚信安全不断助推5G时代的网安技术创新。

网址：www.asiainfo-sec.com　　电话：800-820 8876　　邮箱：lu.di@asiainfo-sec.com

杀毒引擎

产品名称：SAVE 安全智能检测引擎

产品网址：http://www.sangfor.com.cn/product/edr.html



产品介绍

SAVE(Sangfor AI-based Vanguard Engine)是由深信服创新研究院的博士团队联合 EDR 产品的安全专家，以及安全云脑的大数据运营专家，共同打造的人工智能恶意文件检测引擎。该引擎利用深度学习技术对数亿维的原始特征进行分析和综合，结合安全专家的领域知识，最终挑选了数千维最有效的高维特征进行恶意文件的鉴定。相比基于病毒特征库的传统检测引擎，SAVE 的主要优势有:1) 强大的泛化能力，甚至能够做到在不更新模型的情况下识别新出现的未知病毒; 2)对勒索病毒检测达到业界领先的检出率，包括影响广泛的 WannaCry、 BadRabbit 等病毒;3)云+端联动，依托于深信服安全云脑基于海量大数据的运营分析，SAVE 能够持续进化，不断更新模型并提升检测能力，从而形成本地传统引擎、人工智能检测引擎和云端查杀引擎的完美结合。

适用领域

全行业用户。

适用于深信服终端检测响应平台EDR产品针对PC终端，服务器主机，桌面云，云虚拟机的安全防护与文件查杀，深信服下一代防火墙。

公司简介

SANGFOR 深信服科技

公司名称：深信服科技股份有限公司

公司简介：深信服科技股份有限公司是一家专注于企业级安全、云计算及基础架构的产品和服务供应商，拥有智安全、云计算和新IT三大业务品牌，致力于承载各行业用户数字化转型过程中的基石性工作，从而让用户的IT更简单、更安全、更有价值。目前，深信服在全球设有50余个分支机构，公司先后被评为国家级高新技术企业、下一代互联网信息安全技术国家地方联合工程实验室、广东省智能云计算工程技术研究中心等。深信服坚持以持续创新的理念为用户打造省心便捷的产品，获得了市场广泛认可。目前，近10万家用户正在使用深信服的产品。根据IDC数据，深信服硬件VPN、SSL VPN、上网行为管理、广域网优化等多款产品，多年来保持中国市场占有率第一。

网址：http://www.sangfor.com.cn/　　电话：18565862661　　邮箱：thy@sangfor.com.cn

杀毒引擎

产品名称：奇安信 OWL 反病毒引擎(QOWL)

产品网址：https://www.qianxin.com/product/detail/pid/49

产品介绍

奇安信 OWL 防病毒引擎（QI-ANXIN OWL AntiVirus Engine）奇安信历时两年研发的一款自主知识产权的反病毒引擎。简称：QOWL引擎。该引擎具有丰富的格式识别和解析能力、超强的脱壳能力、支持PE和非PE病毒查杀、可完美修复被感染文件、支持高危漏洞的检测、全系统平台（包括移动和国产化）支持、多指令CPU支持、毫秒级扫描速度。

适用领域

个人PC，企业PC，各种服务器发现设备潜在漏洞，显著提高工控设备安全测试效率、降低安全测试成本，帮助工控系统厂商赢取更多的市场占有率。

公司简介

奇安信 新一代网络安全领军者

公司名称：网神信息技术（北京）股份有限公司

公司简介：网神信息技术（北京）股份有限公司（以下简称“网神”）是奇安信科技集团股份有限公司（以下简称“奇安信”）的控股子公司，公司成立于2006年2月，是一家集技术研发、平台管理、综合服务于一体的信息安全产品与服务提供商，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。

奇安信成立于2014年，专门为政府、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，相关产品和服务已覆盖大多数中央政府部门、中央企业和大型银行。

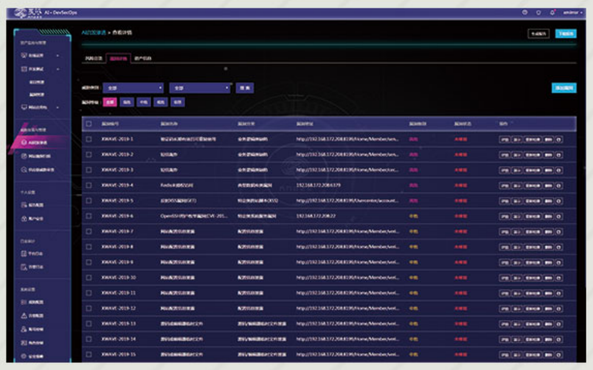
近年来奇安信以高投入研发下的技术创新为引领，特别针对云计算、大数据、移动互联网、工业互联网、物联网等新技术运用下产生的新业态、新场景，为政府与企业等机构客户提供全面有效的网络安全解决方案，率先提出并成功实践“数据驱动安全”“44333”“内生安全”等先进的安全理念，推出了“天狗”系列第三代安全引擎，零信任、“天眼”等创新的安全产品，并于2020年发布面向新基建的新一代网络安全框架，此框架下的"十大工程五大任务"，可以适用于各个应用场景，能指导不同的行业输出符合其业务特点的网络安全架构。

网址：https://www.qianxin.com/　　电话：010-57836300　　邮箱：baizipan@qianxin.com

渗透测试平台

产品名称：悬镜灵脉 AI-IAST 渗透测试平台

产品网址：https://xcheck.xmirror.cn




产品介绍

悬镜灵脉 AI-IAST 渗透测试平台作为悬镜 AI-DevSecOps 智适应威胁管理体系全流程安全赋能平台，通过综合多种流量收集手段（如启发式爬虫、代理、VPN、流量管家、轻量级插桩等）和创新的AI启发技术赋能传统IT从业人员，让政企用户的普通技术员工（研发、测试、运维等）都能完成安全测试和漏洞检测，进而保证安全贯穿于软件开发全生命周期的每一个关键环节，消除上线前的开发安全问题，防止应用带病上线。

灵脉采用AI智适应安全扫描引擎，全方位支持开发生态链安全。灵脉同时支持主动嗅探和AI启发两种漏洞挖掘方式。可协助非安全人员快速完成系统的漏洞挖掘，有效解决传统黑盒扫描方式中爬虫功能的局限性（登录态扫描）问题，还可以深度发现新开发业务系统中存在的各种业务逻辑问题，如水平越权、垂直越权、登录接口爆破、验证码绕过、批量注册等。帮助政企用户快速定位应用漏洞，将安全漏洞的发现和修复时间前置到开发测试环节，大大提升修复效率。

适用领域

灵脉适用于金融、电信、政务、能源、教育、云服务、媒体、交通等各个行业的企事业用户。

公司简介

悬镜 XMIRROR

公司名称：悬镜安全

公司简介：悬镜安全，AI-DevSecOps智适应威胁管理体系开拓者，由北京大学白帽黑客团队“XMIRROR”发起创立，专注于软件供应链全生命周期的高级威胁检测防御，核心业务主要包括AI渗透测试平台“悬镜灵脉”和自适应安全运营平台“悬镜云卫士”等自主创新产品及实战攻防对抗为特色的政企安全服务，为金融、能源、政务、教育及医疗等行业云用户提供创新灵活的智适应安全管家解决方案。

网址：https://www.xmirror.cn　**电话：**010-86469499　**邮箱：**gaoxl@anpro-tech.com

数据安全

产品名称：美创数据脱敏系统

产品网址：http://www.mchz.com.cn/cn/products/index_256.html

产品介绍

美创数据脱敏系统是一款面向敏感数据通过脱敏规则进行数据变形，实现敏感信息的可靠保护的数据脱敏产品。实现自动化发现源数据中的敏感数据，并对敏感数据按需进行脱敏规则变形，避免敏感数据泄露，同时，脱敏后的数据保持了数据的一致性和业务的关联性，应用于开发测试环境、数据交换、数据分析、数据共享等场景。

核心功能：1.主动发现并梳理敏感数据，并匹配脱敏规则；2.按需创建数据源子集及抽取的数量；3.自动同步表结构、主键、索引、约束、外键、函数、存储过程等；4.轻松应对异构数据库脱敏；5.巧设黑名单机制过滤不需要脱敏数据源；6.动态化监控脱敏作业(如:实施脱敏处理效率、单个作业进度等)；7.监控系统运行服务器性能(如:CPU、内存、存储I/0、网络等)。

适用领域

美创数据脱敏系统囊括了各行各业对数据脱敏的主流需求，可广泛应用于众多行业的众多应用场景。不仅可以用在政府、通信、医疗、社保、公安、电力、交通等行业，也可以用在对数据脱敏有着较为硬性和苛刻要求的金融行业。

公司简介

美创 MEICHUANG

公司名称：杭州美创科技有限公司

公司简介：杭州美创科技有限公司（简称“美创科技”）是国内领先的数据安全管理服务的提供商，由多名数据库技术专家携手创办，致力于围绕数据安全、容灾、集成、运维、分析等多方面挖掘和铸造数据价值。总部位于杭州，在北京、广州、南京、成都、武汉等在全国20个省市建立了分支机构，形成了全国化服务网络布局。

美创科技是国内最早一批提出敏感数据防护的国家高新技术企业，实践创新“零信任数据安全架构”，打造了全面涵盖外部威胁防御、内部风险控制、数据追责溯源、数据共享与交换、云安全、业务连续性、运维安全、数据治理、主动运维、大数据应用等一站式全方位的数据安全解决方案，协同腾讯智慧安全、匠迪科技、博越信息等，实现了对网络安全、数据安全、业务安全、运维安全等多领域的覆盖，共建信息安全产业生态圈。

网址：www.mchz.com.cn　　电话：0571—28236100　　邮箱：dingna@mchz.com.cn

数据安全

产品名称：天空卫士内部威胁管理平台

产品网址：http://www.skyguard.com.cn/ITMPage.html

产品介绍

天空卫士内部威胁管理（ITM）技术基于这些海量数据的分析，对内部用户的异常行为或内部威胁进行预测，直接以“人”的视角给出判定，抓住“坏人”、主动出击，在数据泄漏之前进行阻止，并为安全分析人员提供可靠的依据。内部威胁管理（ITM）：采用最先进的统计学异常分析、双向循环神经网络、大数据分析、 贝叶斯信念网络等技术对用户行为特征进行深度建模，发现内部风险行为和异常行为，将用户风险评分结果与基于内容安全引擎策略集成，实现对风险用户进行智能化、实时监督和控制。系统主要包含：分布式的海量日志聚合技术、拓扑感知式的日常探索技术和基于机器学习的安全分析技术。

适用领域

目标用户：政府、运营商、金融、能源、互联网及其他特殊行业。

适用领域：内部威胁防护和管理，企业数据安全保护。

公司简介

天空卫士 SkyGuard

公司名称：北京天空卫士网络安全技术有限公司

公司简介：天空卫士是一家以人工智能技术为核心、以ITP（内部威胁防护体系）技术为基础的新安全技术企业，在数据安全、WEB安全、邮件安全、移动安全和接入云安全等领域开展深入研究和研发，拥有目前国内领先的内部威胁防护技术研发团队，已完成旗舰品牌“SecGator 安全鳄”系列新数据安全产品的研发与发布，并在政府、运营商、金融、能源、互联网及其他特殊行业广泛部署应用，帮助用户有效应对APT攻击、钓鱼信息、内部数据窃取等威胁，实现企业核心数据资产的智能和实时保护。

网址：www.skyguard.com.cn　**电话：**010-50927291　**邮箱：**panlun@skyguard.com.cn

威胁情报

产品名称：暗网空间测绘雷达系统

产品介绍

暗网空间测绘雷达系统是知道创宇推出的全球首款针对暗网空间进行全方位监测的应用系统，通过自研的暗网爬虫引擎和机器学习语言识别算法，以及基于人工智能的内容识别和语义识别引擎，实现了对Tor洋葱网络、I2P网络、ZeroNet等常见暗网协议进行识别、爬取、监控、检索等功能，并依托于ZoomEye的网络空间测绘和指纹识别技术，对整个暗网空间的资产进行发现、抓取、识别和分析，例如组件、端口、指纹、漏洞、隐私泄露情况等，帮助相关部门对暗网空间的节点分布、服务情况、敏感内容、犯罪舆情等情况等进行全方位监测，并可以结合知道创宇的漏洞雷达、攻击雷达等产品模块进行暗网空间的攻击、取情、定位等工作，以达到帮助相关单位部门对暗网空间进行监测、分析、治理的目的。

适用领域

企业、政府、网络监管机构、网信办、公安、国安、军队等。

公司简介

知道创宇

公司名称：北京知道创宇信息技术有限公司

公司简介：知道创宇由数位国际顶尖的安全专家创办，并拥有近百位国内一线安全人才作为核心安全研究团队，长期为政府及企业提供国际先进的网络安全解决方案。知道创宇擅长全新形势下的网络攻防一体技术、产品研发。利用在云计算及大数据处理方面的行业领先能力，为客户提供具备国际一流安全技术标准的可视化解决方案，提升客户网络安全监测、预警及防御能力。公司技术实力受到国家公安部、国务院中央政府采购网、工信部、CNNVD、央行、香港赛马会、微软、浙江卫视等知名客户的强烈认可。

网址：www.knownsec.com　　电话：010-57076191　　邮箱：wangh4@knownsec.com

移动终端安全

产品名称：腾讯手机管家

产品网址：m.qq.com

产品介绍

腾讯手机管家是腾讯旗下一款永久免费的手机安全与管理软件。功能包括病毒查杀、骚扰拦截、软件权限管理、手机防盗及安全防护，用户流量监控、空间清理、体检加速、软件管理等高端智能化功能。以成为“手机安全管理软件先锋”为使命，其“有实力，无所惧” 为产品创新理念，更是成为95后年轻人的性格标签，完美贴合了“信息时代的优先体验者”90后一代时尚新潮的追求。腾讯手机管家，不仅是安全专家，更是用户的贴心管家。

适用领域

全领域。

公司简介

腾讯手机管家 有实力 无所惧

公司名称：腾讯科技（深圳）有限公司

公司简介：腾讯科技（深圳）有限公司成立于1998年11月，是目前中国最大的互联网综合服务提供商之一，也是中国服务用户最多的互联网企业之一。腾讯一直秉承一切以用户价值为依归的经营理念，始终处于稳健、高速发展的状态。

网址：m.qq.com 电话：18611728112 邮箱：frejazhang@tencent.com

云安全

产品名称：京东云 Network Fast 1 应用交付控制器

产品网址：https://www.jdcloud.com/cn/products/nf1-adc

产品介绍

京东云Network Fast 1应用交付控制器包括四大核心功能组件，即：NF1-LTC应用安全防护与负载均衡、NF1-GTC全局流量调度、NF1-TP网络层DDoS防护、NF1-Ctrlcenter流量管理平台。

NF1-LTC组件提供全流程的应用交付能力，包括应用负载、应用优化、应用加速，同时针对应用层攻击提供检测与防护，帮助客户增强应用层威胁抵御能力，NF1-TP组件可针对常见的网络层DDoS攻击进行检测和防护，并提供私有化部署形态，使客户业务的交付效率得到持续的改善和提升。

NF1-GTC组件采用了高性能DPDK转发的设计，可进行权威DNS解析、链路质量监控和全局流量调度，有效避免单点故障，利用GSLB特性可提升混合云场景的业务可靠性，利用京东云安全DNS防御体系，能有效解决DNS劫持、缓存投毒的问题。

NF1-Ctrlcenter组件可实现集中管理与展示，通过Ingress特性能够与云原生容器集群（K8S）、微服务架构、Serverless函数计算集群无缝适配，实现跨平台、跨边界的多云一体化管理和集中分析与展示，帮助客户提升安全管理效率，降低运维复杂度，实现“单点接入，全网可达”的集中式管理。

适用领域

行业用户，包括但不限于政府网站，金融，电商，互联网，游戏等。

公司简介

京东云

公司名称：京东云计算有限公司

公司简介：京东云（JD Cloud）是京东集团旗下的全平台云计算综合服务提供商，拥有全球领先的云计算技术和丰富的云计算解决方案经验。京东云提供从IaaS、PaaS到SaaS的全栈式（Full Stack）服务，包含公有云、私有云、混合云、专有云在内的全场景（Full Services）服务，从IDC业务、云计算业务到综合业务的全频段（Full Spectrum）服务，京东云还致力于为合作伙伴提供覆盖全行业应用、为全行业提供平台支撑的全生态（Full Ecosystem）服务。同时，京东云依托京东集团在云计算、大数据、物联网和移动互联网应用等多方面的长期业务实践和技术积淀，形成了从基础平台搭建、业务咨询规划，到业务平台建设及运营等全产业链的云生态格局，为用户供一站式全方位的云计算解决方案。

网址：https://www.jdcloud.com **电话：**15801616919 **邮箱：**Liyang65@jd.com

云产品

产品名称：京东云 DDoS 防护和流量调度系统

产品网址：https://www.jdcloud.com/cn/products/anti-ddos-pro

产品介绍

京东云DDoS防护和流量调度系统是依托京东云安全团队在京东商城多年攻击防护实战经验之上推出的一款安全产品。旨在用户遭受大流量的DDoS攻击的情况下确保用户业务不中断。产品能够应对的攻击类型包括：协议漏洞攻击、扫描窥探、syn-/ack/udp fragment/icmp Flood、IP Spoofing、http get/post/CC/slow header、SSL DoS/DDoS、TCP连接耗尽/重传/空连接、Sockstress、SIP flood等。无缝适配复杂业务场景需求，单点支持1.5T清洗容量，全网服务稳定性高达99.9999%以上。

京东云以安全合规为指导思想，构建安全研究、安全产品、安全服务、安全治理、安全运营五大体系，建立了集主动风险感知、智能协同防御、多维关联分析和溯源取证于一体的安全管理闭环。基于“平台+能力”的联动能够实现人、机器、数据、情报的无缝连接，大数据分析与威胁情报的智能关联能够自动化完成安全事件分析响应、工单分发、流转、跟踪与闭环。“把安全做到极致，则会变成隐形”。成为客户的隐形保护伞，使客户聚焦于业务的发展，提升客户业务竞争力是京东云安全的首要责任!

适用领域

受DDoS威胁的各行各业用户，包括但不限于政府网站，金融，电商，互联网，游戏等。

公司简介

京东云

公司名称：京东云计算有限公司

公司简介：京东云（JD Cloud）是京东集团旗下的全平台云计算综合服务提供商，拥有全球领先的云计算技术和丰富的云计算解决方案经验。京东云提供从IaaS、PaaS到SaaS的全栈式（Full Stack）服务，包含公有云、私有云、混合云、专有云在内的全场景（Full Services）服务，从IDC业务、云计算业务到综合业务的全频段（Full Spectrum）服务，京东云还致力于为合作伙伴提供覆盖全行业应用、为全行业提供平台支撑的全生态（Full Ecosystem）服务。同时，京东云依托京东集团在云计算、大数据、物联网和移动互联网应用等多方面的长期业务实践和技术积淀，形成了从基础平台搭建、业务咨询规划，到业务平台建设及运营等全产业链的云生态格局，为用户供一站式全方位的云计算解决方案。

网址：https://www.jdcloud.com　电话：15801616919　邮箱：Liyang65@jd.com

云安全

产品名称：京东云态势感知与安全运营中心

产品网址：https://www.jdcloud.com/cn/products/situation-awareness

产品介绍

京东云态势感知与安全运营中心通过收集各安全组件的海量数据，通过大数据关联分析、机器学习、人工智能、高级用户行为分析等技术从全局视角提升对安全威胁的发现识别、理解分析、响应处置，最终为用户提供安全决策的支持。突破传统的增量修补、局部治理和被动防御思路的瓶颈，为用户打造动态的纵深安全防御体系。

产品具备以下功能：安全感知能力，通过收集云上安全组件全面感知已知和未知威胁；安全理解能力，通过云上安全组件提供的海量日志，从中关联分析出安全运维人员能理解的安全事件；安全预测能力，通过机器学习、深度学习和AI技术，预测云上资产将要发生的威胁；告警管理能力，对告警的收集、展示和响应，提升告警的质量，减少告警的数量；工单管理能力，实现安全团队协同化、流程化地进行告警处置与响应，并且确保响应过程可记录、可度量、可考核；案件管理能力，帮助用户对一组相关的告警进行流程化、持续化的调查分析与响应处置，从而持续化地对一系列安全事件进行追踪处置。

自动化编排能力，通过 API或手动的方式，将安全产品、安全能力等组件按照一定的逻辑关系组合到一起，用以完成某个特定安全操作的过程。比如将安全组防火墙、入侵检测/防护、数据库审计、IP高防、WAF、主机安全和威胁情报或大数据平台整合起来，实现自动化安全事件响应和处置。

适用领域

行业用户，包括但不限于政府网站，金融，电商，互联网，游戏等。

公司简介

京东云

公司名称：京东云计算有限公司

公司简介：京东云（JD Cloud）是京东集团旗下的全平台云计算综合服务提供商，拥有全球领先的云计算技术和丰富的云计算解决方案经验。京东云提供从IaaS、PaaS到SaaS的全栈式（Full Stack）服务，包含公有云、私有云、混合云、专有云在内的全场景（Full Services）服务，从IDC业务、云计算业务到综合业务的全频段（Full Spectrum）服务，京东云还致力于为合作伙伴提供覆盖全行业应用、为全行业提供平台支撑的全生态（Full Ecosystem）服务。同时，京东云依托京东集团在云计算、大数据、物联网和移动互联网应用等多方面的长期业务实践和技术积淀，形成了从基础平台搭建、业务咨询规划，到业务平台建设及运营等全产业链的云生态格局，为用户供一站式全方位的云计算解决方案。

网址：https://www.jdcloud.com **电话：**15801616919 **邮箱：**Liyang65@jd.com

产品名称：京东云应用安全网关

产品网址：https://www.jdcloud.com/cn/products/application-security-gateway

产品介绍

京东云安全-应用安全网关是基于京东云高性能负载均衡集群的Web应用安全防护产品，使用京东云Web安全攻击引擎检测、威胁情报联动、AI行为分析、AI攻击检测等多种技术；在京东云VPC网络环境中提供OWASP Top 10 Web安全威胁防护、封禁管理、CC攻击防护、BOT程序管理和网站合规保护等功能。提供便捷的部署、使用体验，兼容普通用户和专家用户，提供丰富的可视化报表，快速感知安全威胁。保护京东云用户的Web应用或API免遭当前和未来的安全威胁，保障用户安全上云。

适用领域

京东云所有有Web业务的用户，VPC东西向和南北向防护。

公司简介

京东云

公司名称：京东云

公司简介：京东云（JD Cloud）是京东集团旗下的全平台云计算综合服务提供商，拥有全球领先的云计算技术和丰富的云计算解决方案经验。为用户提供从IaaS、PaaS到SaaS的全栈式服务（Full Stack），从IDC 业务、云计算业务到综合业务的全频道服务（Full Spectrum），以及包含公有云、私有云、混合云、专有云在内的全场景服务（Full Services）和跨行业的全生态云服务（Full Ecosystem）。同时，京东云依托京东集团在云计算、大数据、物联网和移动互联网应用等多方面的长期业务实践和技术积淀，形成了从基础平台搭建、业务咨询规划，到业务平台建设及运营等全产业链的云生态格局，为用户提供一站式全方位的云计算解决方案。

网址：https://www.jdcloud.com/　　电话：010-56348289　　邮箱：zhangzhishao@jd.com

主机安全

产品名称：腾讯云主机安全

产品网址：www.cloud.tencent.com/product/cwp

产品介绍

主机安全（Cloud Workload Protection，CWP）基于腾讯安全积累的海量威胁数据，利用机器学习为用户提供黑客入侵检测和漏洞风险预警等安全防护服务，主要包括密码破解拦截、异地登录提醒、木马文件检测、高危漏洞检测等安全功能，解决当前服务器面临的主要网络安全风险，帮助企业构建服务器安全防护体系，防止数据泄露。

适用领域

目标用户：拥有腾讯云主机资产，需要主机安全解决方案的企业或个人用户。

适用领域：金融、游戏、泛互联等行业，为主机提供黑客入侵检测、漏洞风险检测等防护服务。

公司简介

Tencent 腾讯

公司名称：腾讯云计算(北京)有限责任公司

公司简介：腾讯云是腾讯倾力打造的云计算品牌，以卓越科技能力助力各行各业数字化转型，为全球客户提供领先的云计算、大数据、人工智能服务，以及定制化行业解决方案。

网址：www.cloud.tencent.com　　电话：4009100100　　邮箱：neotan@tencent.com

主机安全

产品名称：网宿主机入侵检测系统

产品网址：https://www.wangsu.com/product/162

产品介绍

网宿主机入侵检测系统（HIDS）基于网宿平台积累的海量攻击数据，通过部署轻量级的主机探针，结合云端智能分析引擎，为企业主机资产提供覆盖全生命周期的安全威胁监测、分析、预警等安全服务，包括有效识别弱口令、高危漏洞等常见安全风险；实时监测网页后门植入、病毒木马运行、敏感文件篡改等黑客入侵行为，保障主机安全，守护企业数字资产。

适用领域

国企央企，政府单位，金融保险，互联网，能源制造，教育等行业客户在混合环境下的主机安全监测及入侵防护需求。

公司简介

网宿科技

公司名称：网宿科技股份有限公司

公司简介：网宿科技成立于2000年1月，致力于互联网和云计算基础设施等方面的关键技术研究，主要业务是在全球范围提供内容分发网络（CDN）、云安全、云计算、互联网数据中心等服务。公司已在全球搭建了广泛高效的内容分发网络，并持续推进节点下沉、本地覆盖，开发面向边缘计算的支撑平台，以满足未来用户随时随地的数据计算及交互需求。目前，公司服务约3,000家中大型客户，包括互联网企业、政府、传统企业及电信运营商。针对客户在IT部署及数据计算、传输、安全等方面的需求，公司总结多年来服务各行业的经验和行业特点，推出针对视频、手机直播、游戏、电商、媒体、汽车、快消、金融、政务、教育、家电制造等行业的整体解决方案，并为客户提供定制化服务。

网址：www.wangsu.com　　电话：021-24261717　　邮箱：hugw@wangsu.com

主机安全

产品名称：悬镜云卫士专业版

产品网址：http://yws.xmirror.cn/

登录界面


总览界面

产品介绍

悬镜云卫士是由北京安普诺信息技术有限公司研发的一款主机级自适应防黑加固智能安全运维平台。悬镜云卫士可以适应公有云、私有云、混合云及物理机等各种环境，以部署在服务器上的轻量级 agent 为检测探针，通过基于 RNN算法的云脉威胁检测引擎，全面感知威胁行为。XCARTA 自适应引擎可以持续调整信任及风险模型，并智能优选防御策略，使得在保障用户业务稳定高效的同时，最大程度地抵御外部威胁。

产品特点：灵活自适：内置独创的基于机器学习技术的XCARTA引擎，对业务环境的要素持续地做信任及风险评估并调整模型，在保障用户业务的前提下，最大化地输出防护能力。未知威胁：不再单纯依赖传统防火墙、IPS等产品使用的特征匹配，而通过基于RNN算法的云脉威胁检测引擎，对数据进行更加准确细致地威胁元素赋值，从而拥有对未知威胁的识别能力。纵深检测：内置基于攻击链模型的多锚点检测引擎，锚点间数据互联、逻辑互通，协同分析评估威胁，形成恶意行为难以绕过的检测矩阵。全面防御：拥有资产清点、漏洞扫描、基线检测、弱口令、防暴力破解、防端口扫描、异常登录、网站后门、主机木马、异常事件、日志审计等多维度安全能力，全面保护主机安全。

适用领域

适用于：对服务器及主机安全有一定需求的政企终端客户；意愿强化主机安全能力，并计划向用户输出安全能力的云服务商。

可部署于：公有云、政务云、媒体云、教育云、金融云等各种云环境；物理机集群。

公司简介

悬镜 XMIRROR

公司名称：悬镜安全

公司简介：悬镜安全，北京安普诺信息技术有限公司旗下AI智能云安全品牌，由北京大学白帽黑客团队“Xmirror”主导创立，核心产品线包括悬镜云卫士、灵脉AI自动化渗透测试系统等自主创新产品与政企安全服务，专注为媒体云、政务云、教育云、农业云、城市云等政企用户提供创新灵活的自适应云安全管家解决方案。

网址：http://www.anpro-tech.com/ **电话：**010-86469499 **邮箱：**yangmx@anpro-tech.com

赛可达实验室

skd labs

国际知名第三方网络安全服务商

公正　中立　科学　严谨

赛可达实验室官网

微信公众号

北京赛可达信息技术有限公司

北京市海淀区知春路锦秋国际A座1505

info@skdlabs.com

+86(010) 8269 6081

http://www.skdlabs.com