360政企安全

数 字 安 全 的 领 导 者

2022

COMPANY BROCHURE

THE LEADER IN DIGITAL SECURITY

数 字 安 全 的 领 导 者

360政企安全集团

数 字 安 全 的 领 导 者

360
THE
LEADER
IN
DIGITAL
SECURITY

CONTENTS

01. 集团概况 P007-012

02. 安全优势 P013-022

03. 使命愿景 P023-026

04. 数字安全能力体系 P027-032

05. 安全产品与解决方案 P033-054

06. 创新技术落地及实践 P055-072

07.ISC 互联网安全大会 P073-085

360
www.360.cn
安全上网
从360开始

01

集团概况

360政企安全集团，是数字安全的领导者。过去17年专注为国家、城市、行业、企事业单位提供网络安全技术、产品和服务，是国内较早涉足To G To B领域的安全企业之一，目前已与众多部委、央企、大型金融机构、运营商以及上百万中小企业开展了网络安全合作。

360政企安全集团基于十余年在安全大数据、知识库、安全专家方面的积累，已成为唯一掌握全网态势感知、唯一具有17年攻防实战经验的网络安全公司，同时也成为云端安全大脑为核心的数字安全能力体系创立者。

其中，360数字安全能力体系包含新战法、新框架、新技术、新能力。而新框架作为数字安全能力体系的重要组成，包含基础能力框架和八大数字安全框架。基础能力框架以安全大脑为核心，构建了攻击面防御、资源面管控、数据运营、专家运营等4大类基础设施，这些基础设施可以不断扩展，帮助党政军企用户构建一套可运营、可持续、可成长、可输出的安全能力，支撑形成大数据安全、云安全、物联网安全、新终端安全、网络通信安全、供应链安全、应用安全、区块链安全等八大数字安全框架。

基于此，360政企安全集团以数字安全能力体系帮助国家、城市、行业、企事业应对数字时代的安全挑战，践行数字安全领导者担当。

目前，这套体系接连服务于重庆、天津、青岛、鹤壁、苏州、郑州、上海、周口等城市的安全基础设施建设和运营，树立了标志性的城市级安全服务典范，构建起以安全大脑为核心的协同防御体系，整体提升我国应对数字时代高级威胁的安全能力。

除此之外，360政企安全集团也是国家网络安全保障的核心力量，在两会、十九大、九三阅兵、“一带一路”峰会、G20、金砖会议、APEC、七十周年庆典、2022年北京冬奥会等活动的重保工作，以及国家安全和国防安全相关工作中发挥了重要保障作用。

360
THE LEADER IN DIGITAL SECURITY

MILESTONES
大事记

2005

360集团成立

2005年，中国信息安全行业大潮初起，奇虎360科技有限公司正式成立，以为人民服务的愿景，引领中国互联网与安全服务发展的新浪潮。

2008

全球首创免费杀毒模式，彻底颠覆行业格局

正式推出永久免费的360杀毒，完全摈弃了传统杀软固有的“激活码”机制，并以极高的性能指标全面超越全球范围内的收费杀毒软件。

2011

成功挂牌上市

2011年3月，奇虎360正式在纽约证券交易所挂牌上市，证券代码为NYSE：QIHU，并以40倍的罕见超额认购量，成为当年中国企业在美国最成功的IPO交易之一。

2013

打造行业首个亚洲顶级峰会
——ISC互联网安全大会

2013年9月，360重磅打造了行业首个亚洲顶级峰会——ISC互联网安全大会。作为国内规模最大的网络安全盛会，ISC在与会规模、专业度及影响力上均开创了国内信息安全会议的先河。

MILESTONES
大事记

2015

成立360企业安全集团

2015年5月，360宣布正式成立360企业安全集团，专注研制面向政府、企业的新一代网络安全产品和服务，以“互联网+”思维，全面进军企业安全市场。

2016

完成360私有化交易

2016年7月，360正式从纽交所退市回归中国，全力投入国家网络安全建设，捍卫政府部门、外交单位、国防科研院所及银行等机构网络安全。

完成国家级重保项目

先后顺利完成十九大、两会、九三阅兵、一带一路高峰论坛、金砖国家厦门峰会、上合青岛峰会、国际刑警大会等国家级网络安全保卫任务，先后投入3000多人次，昼夜奋战24000小时，处理了上万次应急事件，用安全能力和行动捍卫着国家和企业的网络安全。

2017

全球首发WannaCry勒索病毒检测工具与自救指南

2017年5月12日，美国NSA武器库泄露导致WannaCry勒索病毒全球大爆发，席卷150余个国家，大量政府机构和公共设施瘫痪， 360第一时间紧急预警处置，并全球首发勒索病毒检测工具和自救指南，最终成功保障国内360安全卫士6亿用户上网安全，无一例中招。

MILESTONES
大事记

2018

三六零集团A股上市

2018年2月，三六零完成重组更名，在上海证券交易所实现A股上市，并以“科技股龙头”的强劲冲势，正式成为网络安全“国家队”。

360安全大脑战略布局

360整合十余年沉淀的安全大数据、安全专家、攻防知识库等核心能力，倾力打造网络空间“预警机”和“反导系统”—360安全大脑，开创大安全战略布局，并借此一举荣获第五届世界互联网大会“世界互联网领先科技成果”重磅殊荣。

全球首家捕获 “双杀”漏洞APT攻击

全球首家捕获利用浏览器0day漏洞的新型Office APT攻击，并第一时间紧急预警处置，成功保障国内政府机构、企事业单位免遭损失。

全球首家发现EOS区块链高危安全漏洞

全球首家发现一系列价值千亿美金的EOS区块链高危安全漏洞，并协助完成修复，成功挽救全球区块链数字货币体系免遭网络瘫痪的风暴攻击。

2019

斩断RDP高危漏洞风暴

微软“蠕虫级”RDP远程高危漏洞（CVE-2019-0708）震荡全球。360安全大脑第一时间发布安全预警，并全球独家推出RDP远程漏洞无损扫描工具、远程桌面服务漏洞免疫工具和RDP远程漏洞热补丁工具，保护全网系统免遭漏洞威胁。

发布360政企安全战略3.0

全面升级政企安全战略，应对网络战，构建大安全生态，以“共建、赋能、投资、培训”的发展模式，打造捍卫国家、城市、行业、企事业单位的国之重器。

问鼎微软MSRC安全精英榜

在微软2019年MSRC全球最具价值安全精英榜中，360安全专家的进榜人数和综合排名均位列全球第一：10人荣耀登榜，并包揽榜单前两名；同时一举摘得安全界“奥斯卡”桂冠，拿下最佳提权漏洞奖，成为中国首个The Pwnie Awards大奖得主。

再获“世界互联网领先科技成果”殊荣

“360全视之眼-0day漏洞雷达系统”荣获第六届世界互联网大会“世界互联网领先科技成果”殊荣。

MILESTONES
大事记

2020

全球首家实锤某国情报组织对我国关键领域长达11年的网络攻击

360全球独家实锤披露某国情报组织对我国关键领域长达十一年的渗透网络攻击。截至目前，360已累计捕获47个境外对我国的APT组织，监测到4200多次对我国20000多家重要机构单位的高级网络攻击事件。

更名360政企安全集团

作为国内唯一“国家级”网络安全解决方案公司，360企业安全集团正式升级更名为360政企安全集团，以16载安全之力高位启航，扩大安全生态布局，全面铺开“政+企”战略建设。

2021

首次提出数字安全能力体系

基于17年实战攻防经验总结出一套以“作战、对抗、攻防思维”为指导，将安全体系与数字体系融合，攻防能力与管控能力融合的新战法。基于新战法形成了数字安全能力框架，这套框架包含基础能力框架和八大数字安全框架。这套框架是数字安全能力体系的整体结构，可支撑形成大数据安全、云安全、物联网安全、新终端安全、网络通信安全、供应链安全、应用安全、区块链安全等八大数字安全框架，以体系化的安全解决方案应对数字时代的安全挑战。

360政企安全集团斩获五项大奖

360政企安全集团一举斩获五项大奖——包括“2020中国数字政府领军企业奖”“2020中国数字政府领军人物奖”“2020中国数字政府技术创新奖”“2020中国数字政府优秀服务商”“2020中国数字政府优秀解决方案奖”。

城市实践案例之典范

截至目前，360政企安全集团已接连服务于重庆、天津、青岛、鹤壁、苏州、郑州、周口等多个全国地标城市的安全基础设施的建设和运营，其中360重庆城市安全大脑被IDC评为中国智慧城市安全运营中心典型实践方案，同时荣获2022年IDC亚太区智慧城市大奖（中国区）。

2022

开启数字安全元年

宣布全面转型数字安全公司，一方面通过开放安全能力、实战方法论、数字安全能力体系给行业，为行业发展提供支撑；另一方面，携手行业伙伴，通过数字安全能力框架帮助用户在转型过程中构建安全能力，共同打造数字安全新生态。

360核心安全大脑3.0发布

依托360云端安全大脑以及17年攻防实战积累的安全大数据、攻防对抗知识库、威胁情报等领先能力正式发布360核心安全大脑3.0，帮助构建政企用户的“能力中枢平台”。

360

THE LEADER IN DIGITAL SECURITY

02

安全优势

① 安全大数据

② 安全专家

③ 高级威胁情报

④ 漏洞挖掘与研究

360
GOVERNMENT
AND ENTERPRISE
SECURITY
GROUP

01

SECURITY BIG DATA

安全大数据

360拥有300亿样本数据、22万亿安全日志、90亿恶意域名信息、2EB以上的安全大数据，数据量国内第一；可以瞬间调用超过百万颗CPU参与计算、检索和关联多维度数据，足以在千丝万缕的复杂数据中，进行分析、挖掘，快速发现高级威胁的蛛丝马迹。

全球独有样本库

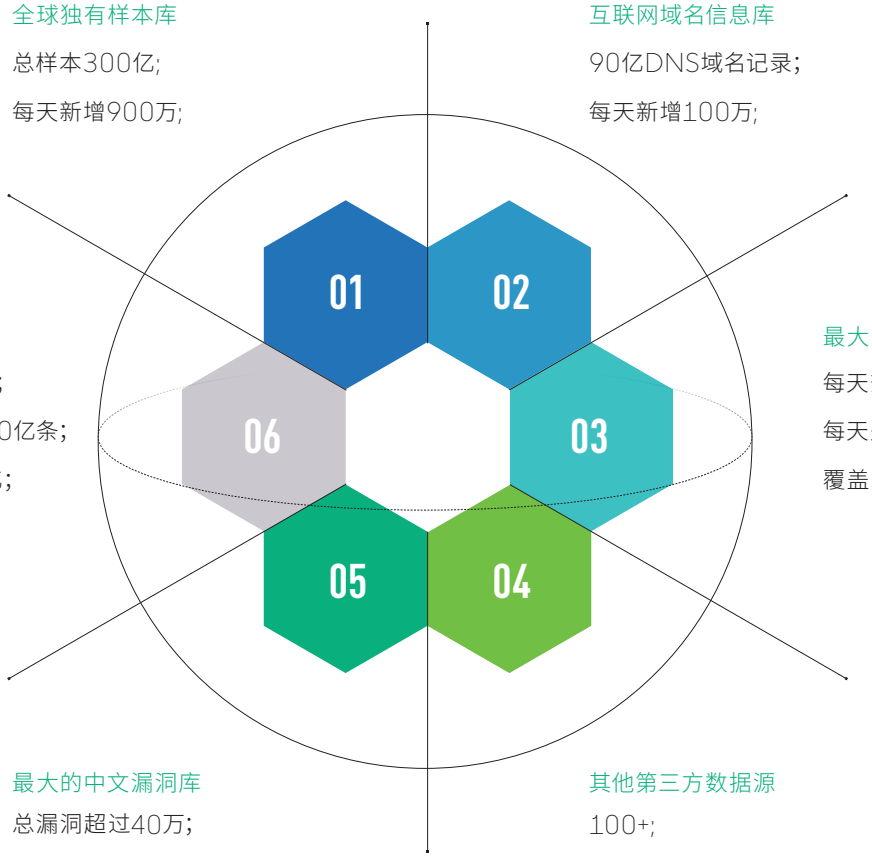
总样本300亿;

每天新增900万;

互联网域名信息库

90亿DNS域名记录；

每天新增100万;



立体式主防库

覆盖5亿客户端；

总日志数50000亿条；

每天新增100亿；

最大的存活网址库

每天查询300亿条;

每天处理100亿条；

覆盖国内96%客户端;

最大的中文漏洞库

总漏洞超过40万；

每天新增可达500个；

其他第三方数据源

100+;

02

SECURITY EXPERTS

安全专家

连续五年 (2017&2018&2019&2020&2021)
封神问鼎MSRC安全精英榜

微软MSRC安全精英榜，表彰和致谢为全球安全事业作出巨大贡献的安全精英，会根据安全精英的研究成果总积分筛选出当年全球排名前5%的安全精英。

2017 MSRC Top100，360公司10人上榜，其中七人排名前50，入选人数和综合排名全面领先。其中360Vulcan团队的YUKI CHEN更是名列全球第三；

2018 MSRC Top100，360公司共有13人荣耀登榜，进榜人数和综合排名都遥遥领先；

2019 MSRC Top100，360公司10人荣耀登榜，其中7人皆在榜单前50，无论入选人数和综合排名，360均位列世界第一；

2020 MSRC Top100，360安全团队共计13名成员荣登最具价值安全精英榜，其中5人位居榜单TOP10，来自360漏洞研究院的3位安全精英更是成功屠榜前三甲；

MSRC 2021 Q1最具价值安全精英榜中，360安全团队的古河 (YUKI CHEN) 以4365分的战绩再次拿下榜首！

2017MSRC

2018MSRC

2019MSRC

2020MSRC

2021MSRC

2018-2020三度蝉联“天府杯”冠军

2018年，360安全团队从100多只队伍中脱颖而出，摘得桂冠。2019年，360一举拿下38.25万美元奖金最高战绩，二度蝉联 “天府杯”冠军，更摘得2019天府杯“最具价值产品破解”奖的重磅殊荣。2020年360凭借多个“全球首破”一举斩获81.25万美金奖励，奖金总数远超其余参赛战队奖金总和，三度称霸天府杯，再夺最具价值产品破解一等奖!

2020年华为终端安全奖励计划一等奖

2020年华为终端安全奖励计划榜单正式发布，360AlphaLab（阿尔法实验室摘得华为终端安全奖励计划一等奖。至此，360AlphaLab位列华为安全奖励计划总榜榜首。

2021首届信创关键产品安全挑战赛

360漏洞研究院在全国各地88支安全战队中脱颖而出， 贡献多个信创基础软硬件漏洞成果，最终成为首届“信创关键产品安全挑战赛”总冠军。

2021谷歌Chrome最具价值安全精英榜

360政企安全集团六名安全精英跻身榜单，入选人数和综合排名全球第一! 来自360 漏洞研究院的李超摘得榜首，成为谷歌Chrome漏洞奖励计划排名最高的中国安全研究员。

0	Leecraso(@leecraso) of 360 Vulnerability Research Institute
1	Khalil Zhani
2	Rory McNamara
3	David Erceg
4	Cassidy Kim of Amber Security Lab, OPPO Mobile Telecommunications Corp. Ltd.
5	Weipeng Jiang (@Krace) from Codesafe Team of Legendsec at Qi'anxin Group
6	Yangkang (@dnpushme) of 360 ATA
7	raven (@raid_akame)
8	Nan Wang (@eternalsakura13) and koocola (@alo_cook) of 360 Vulnerability Research Institute
9	Rong Jian(@__R0ng) of 360 Vulnerability Research Institute
10	ZhanJia Song
11	Zhong Zhaochen
12	Anonymous
13	Brendon Tiszka

【16个研究团队】

- 360 Vulcan Team
- 360 Vulpecker Team
- 360 Sky-Go Team
- 360 0kee Team
- 360 Alpha Lab
- 360 Nirvan Team
- 360 Gear Team
- 360 QVM Team
- 360 MeshFire Team
- 360烽火实验室
- 360高级威胁应对团队
- 360冰刃实验室
- 360NetLab
- 360白泽实验室
- 360诺亚实验室
- 360 Helios Team

【8个研究机构】

- 360天枢智库
- 360工业互联网安全研究院
- 360网络安全研究院
- 360数据安全研究院
- 360安全工程研究院
- 360AI安全研究院
- 360云安全研究院
- 360标准化部

【4大国家工程实验室/研究中心】

- 大数据协同安全技术国家工程研究中心
- 大数据分析与应用技术国家工程实验室
- 计算机病毒防治技术国家工程实验室
- 网络事件预警和防控技术国家工程实验室

03

ADVANCED THREAT INTELLIGENCE

高级威胁情报

多类型情报整合

可对十多个维度线索进行精细化提取、分离、关联、索引，并通过可视化模型综合分析样本，对安全攻击行为进行全面立体化溯源。

商业情报

通过情报交换和情报采购，360整合全球多家厂商的IOC，通过平台运营获得价值较高的情报信息。

开源情报

通过第三方开源平台获取全球最新情报，通过平台对情报进行对比、分析、关联、聚合，得到价值较高情报信息。

自研情报

通过360内部多个团队在安全活动中的运营情况，整合移动端、物联网端、WEB端、服务器端、PC端等多种安全日志汇聚成高质量的IOC情报。

高级情报

通过360多个核心团队的安全活动可产出高价值的不同情报，涉及高级威胁事件、全球范围内的网络攻击活动、国内黑灰产等攻击活动、对外高级威胁组织研究等高价值情报。

360 APT全景雷达

目前360已累计发现CIA、海莲花、摩诃草、美人鱼等境外APT组织50个，以“看见”网络攻击、威胁的能力，严守国家第一道网络安全防线，全面守护网络空间安全。

盲眼 (APT-C-36)

军刀狮组织 (APT-C-38)

Darkhotel (APT-C-06)

蔓灵花 (APT-C-08)

双尾蝎 (APT-C-23)

摩诃草组织 (APT-C-09)

海莲花 (APT-C-00)

沙虫 (APT-C-13)

白金(APT-C-30)

美人鱼组织 (APT-C-07)

方程式(APT-C-40)

拍拍熊组织 (APT-C-37)

黄金雕 (APT-C-34)

毒针(APT-C-31)

ScarCruft(APT-C-28)

肚脑虫组织 (APT-C-35)

人面狮(APT-C-15)

毒云藤(APT-C-01)

Lazarus(APT-C-26)

CIA(APT-C-39)

ArmaRat(APT-C-33)

黄金鼠(APT-C-27)

APT28(APT-C-20)

Carbanak(APT-C-11)

索伦之眼(APT-C-16)

蓝宝菇 (APT-C-12)

Turla(APT-C-29)

.....

04

VULNERABILITY DISCOVERY AND RESEARCH

漏洞挖掘与研究

至今为止，360安全团队累计挖掘主流厂商CVE 漏洞超过2000个，包揽苹果、谷歌、微软三大巨头漏洞挖掘史上最高奖金，实现大满贯，实力领跑全球。

Google

“梯云纵”漏洞获得史上最高奖金

(201,337美元)

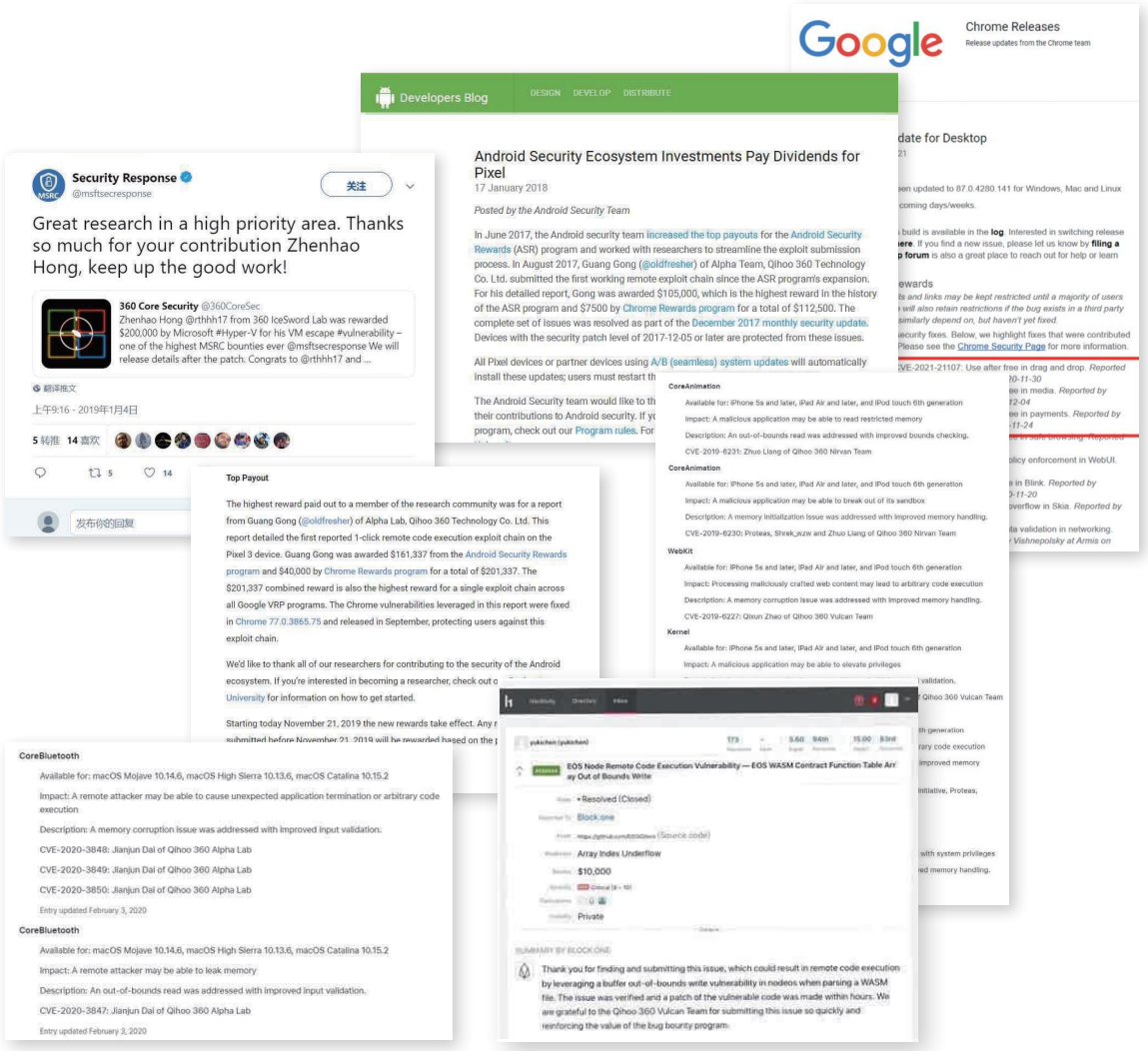
“远程越狱”系列漏洞获得史上最高奖金

(200,000美元)

Microsoft

“虚拟机逃逸”漏洞获得史上最高奖金

(200,000美元)



- 360安全大脑发现并协助微软修复“虚拟机逃逸”漏洞，获微软官方致谢！
- 360安全大脑梅开二度，凭“梯云纵”漏洞，获谷歌史上最高奖金并获官方致谢！
- 360安全大脑发现并协助苹果修复“Bluewave”漏洞，获苹果致谢！
- 360安全大脑独家发现Chrome四大“高危”漏洞，360再获谷歌官方致谢！
- 360安全大脑发现并协助谷歌修复“穿云箭”漏洞，获谷歌官方致谢！
- 360安全大脑发现并协助苹果修复远程越狱系列漏洞，包揽大满贯！
- 360安全大脑发现并协助修复EOS安全漏洞，获EOS致谢！

360

THE LEADER IN DIGITAL SECURITY

03

使命愿景

360政企安全集团经过多年在安全大数据、知识库、安全专家等方面的积累，成为了唯一掌握全网安全态势的网络安全公司、唯一具有17年攻防实战经验的网络安全公司及以云端安全大脑为核心的能力体系创立者，守护国家、城市、行业、企事业的安全。

360
GOVERNMENT
AND ENTERPRISE
SECURITY
GROUP

360政企安全集团三大“能力位”

唯一掌握全网安全态势的网络安全公司

唯一的商业模式：免费杀毒

17年为网民和国家的服务造就云端安全大脑

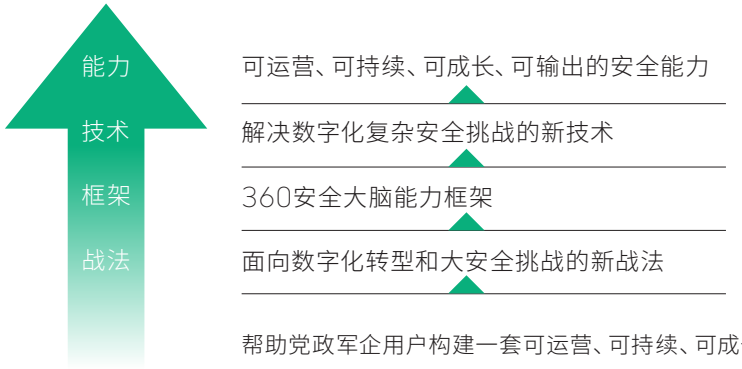
- 最大的程序文件样本库
  总样本数300亿+
- 最广的存活网址库
  每天50000亿条活跃网址访问记录
- 最全的程序行为日志库
  总日志数22万亿条
- 最新的全球域名信息库
  全球90亿域名信息

唯一具有超17年攻防实战经验的网络安全公司

打造基于实战的安全规划建设方法论

以云端安全大脑为核心 的能力体系创立者

面向未来的数字安全能力体系



帮助党政军企用户构建一套可运营、可持续、可成长、可输出的安全能力

四大使命

01.国家安全

360全面守护国家网络空间安全
数年间发现并定位多起境外高级黑客组织对我国发起的网络攻击

360政企安全集团在过去数年发现了50个境外的APT组织；
2020年共披露了23个APT组织涉及全球范围的攻击活动；
2020年共披露13个针对我国发起攻击的APT组织，首次披露的组织8个，如魔鼠、蓝色魔眼和旺刺等；
2021年上半年共捕获15个针对我国发起攻击的APT组织，首次发现的组织4个：芜琼洞、伪猎者、腾云蛇、APT-C-62；
挖掘苹果、谷歌、微软主流厂商CVE漏洞超过2000个，并包揽三大巨头史上最高奖金，实现大满贯；
监测到4200多次对我国20000多家重要机构单位的高级网络攻击事件。

02.城市安全

360为城市构建数字经济安全底座

建设运营中：重庆、天津、青岛、鹤壁、苏州、郑州、上海、周口……
规划建设中：北京、成都、洛阳、沈阳、西安……
城市安全大脑建设，现已覆盖四大直辖市，渗透部分省会城市
未来将逐步全面覆盖省会城市，并往地级市逐步延伸

03.行业安全

建设行业级安全大脑体系

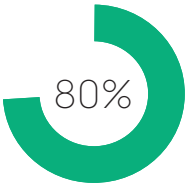
360行业安全大脑为各行各业数字化转型保驾护航
最终构建出一个分布式的、覆盖全国的
“行业安全大脑体系”

- 工业安全大脑
- 国土安全大脑
- 党务安全大脑
- 国防安全大脑
- 医疗安全大脑
- 广电安全大脑
- 政务安全大脑
- 能源安全大脑
- 金融安全大脑
- 关基安全大脑
- 运营商安全大脑
- 网信安全大脑
- 交通安全大脑
- 文化安全大脑
- 汽车安全大脑
- …行业安全大脑

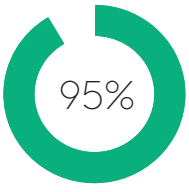
04.企事业安全

建设本地安全大脑，完成一站式安全运营

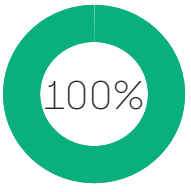
中央部委覆盖率



央企覆盖率



大型金融机构覆盖率



运营商覆盖率

360

THE LEADER IN DIGITAL SECURITY

04

数字安全能力体系

为解决数字化的复杂安全挑战，360政企安全集团沉淀形成了面向数字化的新战法、新框架、新技术、新能力，并打造了数字安全能力体系，帮助党政军企用户构建一套可运营、可持续、可成长、可输出的安全能力。360政企安全集团以数字安全能力体系帮助国家、城市、行业、企事业应对数字时代的安全挑战，践行数字安全领导者担当。

360
GOVERNMENT
AND ENTERPRISE
SECURITY
GROUP

面向未来的数字安全能力体系

面向未来的数字化安全能力体系建设需遵循“四新”原则，可持续性的闭环输出全体系数字化安全能力

01 新战法

以「三化六防」为指导，立足系统思维
安全体系与数字体系融合，攻防能力与管控能力融合

一个指导

以「三化六防」为指导

两个融合

立足系统思维安全体系与数字体系融合

攻防能力与管控能力融合

02 新框架

把360安全大脑能力框架复制给党政军企用户
构建一套可运营、可持续、可成长、可输出的安全能力

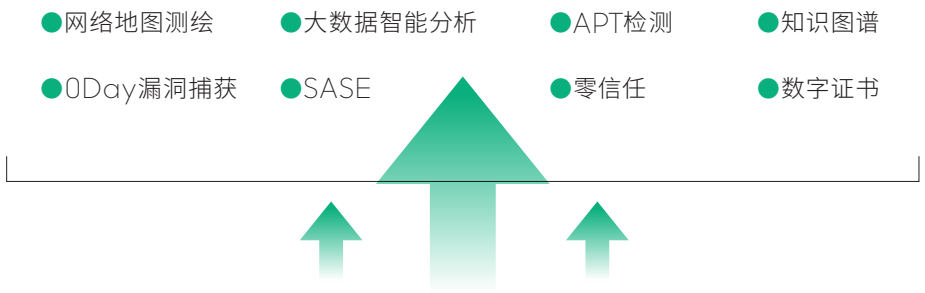
八大安全框架

- 新终端安全
- 物联网安全
- 大数据安全
- 应用安全
- 供应链安全
- 区块链安全
- 云安全
- 通信与网络安全

基础能力框架

03 新技术

新技术运用于新框架，解决数字化时代的复杂安全问题



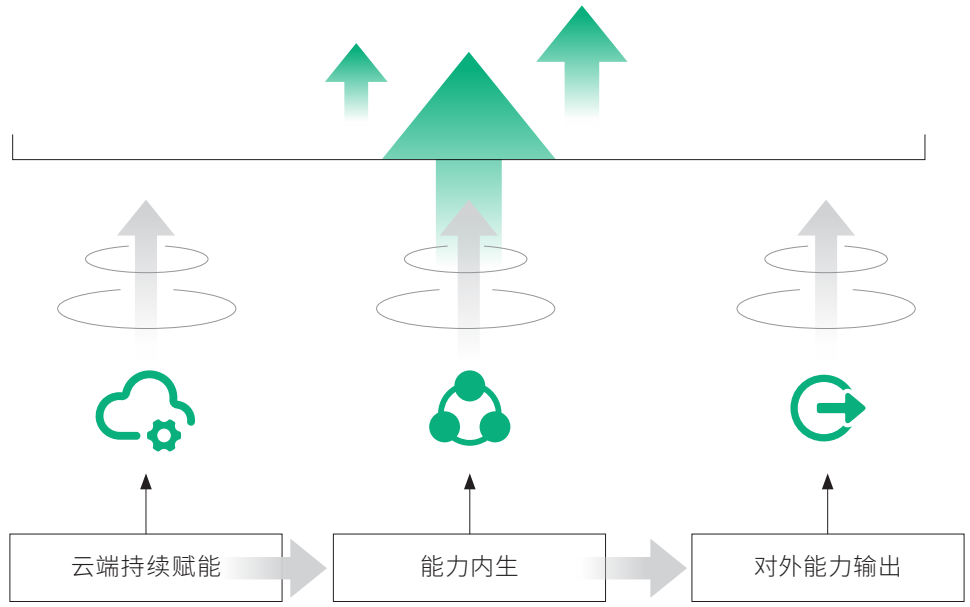
360安全大脑能力框架

基于安全大脑能力框架持续补充新技术，应对复杂挑战

04 新能力

以数据和专家为支柱、以攻击面防御和资源面管控为利器、以安全大数据平台为基础、以安全大脑为核心的安全架构

把360安全大脑能力框架复制给党政军企用户
构建一套可运营、可持续、可成长、可输出的安全能力



能力生成

基于安全大脑的数字安全能力框架

八大安全框架

新终端安全	物联网安全	大数据安全	云安全
应用安全	通信与网络安全	供应链安全	区块链安全

基础能力框架

专家运营基础设施

安全运营　应急响应　人才培养　能力评估　安全开发

攻击面防御基础设施

网络攻防靶场

漏洞管理

攻击诱捕

高级威胁检测

API安全管理

资源面管控基础设施

密码/证书

安全访问服务边缘

身份管理

零信任

区块链安全

安全大数据平台

数据运营基础设施

知识图谱　态势感知　威胁情报　网络空间测绘

流量检测与响应　终端检测与响应　DNS检测与响应

360

THE LEADER IN DIGITAL SECURITY

360
GOVERNMENT
AND ENTERPRISE
SECURITY
GROUP

360

THE LEADER IN DIGITAL SECURITY

05

安全产品与解决方案

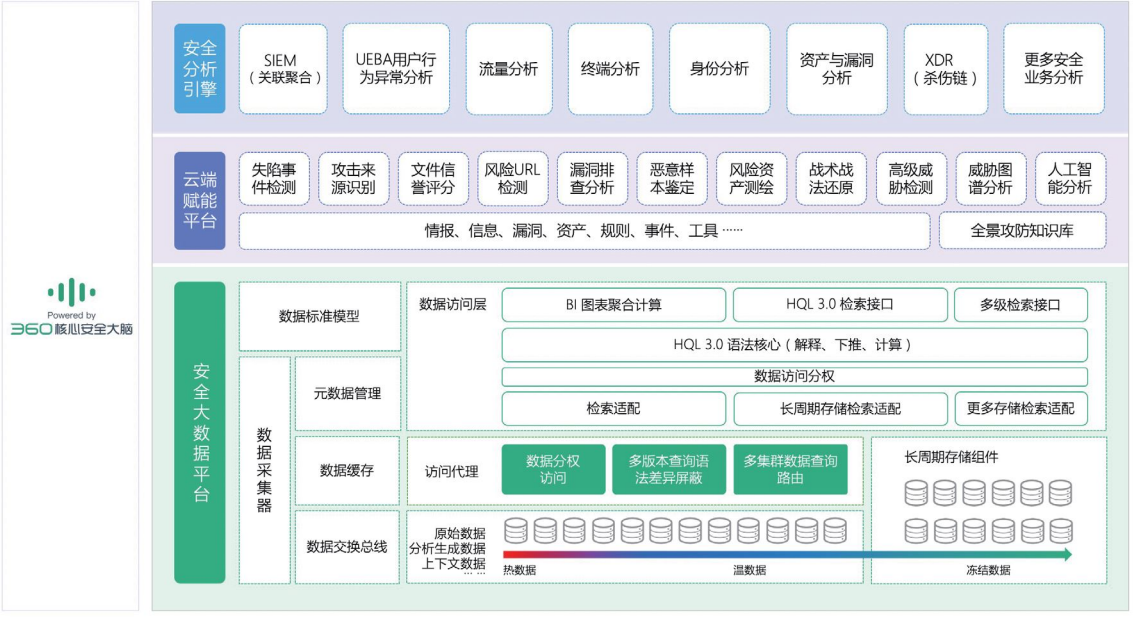
① 5.1 360核心安全大脑
② 5.2 安全产品全景图
③ 5.3 重点安全产品
④ 5.4 安全服务
⑤ 5.5 解决方案

360
GOVERNMENT
AND ENTERPRISE
SECURITY
GROUP

5.1 | 360核心安全大脑 | SECURITY PRODUCTS

概述

360核心安全大脑作为面向未来的数字化安全能力体系中的“中枢系统”负责全面体系化的核心运算及分析工作，通过联动“云端安全大脑”全面赋能360以及合作伙伴生态内的所有安全产品，从架构上打破云端知识、客户业务及生态数据之间的固有屏障，拓展全局安全视野，融通各类安全数据，协同整体实战决策；帮助相关安全产品在信息共享的全面覆盖、大数据集中分析研判、高级威胁情报赋能、网络安全产品体系化联动等全方面提升业务能力，帮助用户大幅度提升安全风险的识别、保护、检测、响应、恢复等各项能力。



架构示意图

360
GOVERNMENT
AND ENTERPRISE
SECURITY
GROUP

360核心安全大脑3.0由一个安全大数据平台、一个云端赋能平台和多个安全分析引擎，以及内嵌360十七年经验所积累的实战方法论组成:

安全大数据平台吸收360在搜索引擎研发积累的多年经验，通过模型化管理的数据标准，接入各类安全数据使之集中管理，并在内部融合数据品类，协调数据流程决策与步骤，为安全业务提供从数据接入到存储、清洗到运算，最终到图表展示的全生命周期一站式服务。

安全大数据平台具有“运营商”级别的数据处理能力，内置解析规则支持接入200+厂商，2000+数据源，输出多达1200+解析维度，丰富度远超友商，是业界数据解析最规范和全面的平台。

云端赋能平台依托360云端强大的安全大数据实力，云地协同、能力下沉，为安全设备提供从漏洞到资产、从情报到知识、从线索到规则、从事件到态势等100余种基础的安全数据及分析能力，可以满足各类安全设备的通用化威胁检测与分析需求，如: 失陷事件检测、攻击来源识别、恶意样本鉴定、风险URL检测、漏洞排查分析、文件信誉评分、风险资产测绘、战术战法还原、高级威胁检测、威胁图谱分析、人工智能分析等。

云端赋能平台是360十七年2EB海量安全大数据(其中包括180+亿恶意网址、5万亿+存活网址、样本文件300亿+、DNS解析记录700亿+等)积累的本地化实例，既包含了与全球高级别攻击对手持续十余年的网络实战对抗经验，又包含了360总结出的攻防对抗知识库、APT组织知识库、漏洞知识库、病毒库等多维度全景攻防知识库，助力客户建立“知其然，更知其所以然”的数据分析体系。

结合特定安全业务场景，配合专用安全设备，多个专用的安全分析引擎可以把专业的分析能力通过配置组合的方式赋能特定的安全产品，如: 聚合关联事件分析、用户异常行为分析、威胁流量还原分析、终端威胁线索分析、网站威胁监测分析、数字资产风险分析等专用能力。

安全分析引擎预置了10大类，60余小类，2000多个安全策略，应对纷繁复杂的安全业务，可灵活组合、相互补充、协同联动，从多个维度指导安全设备发现、防护高级别网络威胁，提升自身网络安全能力。

5.2 | 安全产品全景图 | SECURITY PRODUCT PANORAMA

01 攻击面防御基础设施群

攻击诱捕基础设施

360 攻击欺骗防御系统

漏洞管理基础设施

360 漏洞云安全众测服务平台
360 漏洞情报平台
360 资产脆弱性扫描平台

实网攻防靶场平台基础设施

360 网络攻防靶场平台
360 新一代实网攻防靶场平台
360 安全运维管理系统
360 网络攻防训练平台
360 网络攻防竞赛平台

02 数据运营基础设施群

终端检测与响应基础设施

360 终端安全管理系统
360 终端安全管理系统（一体化版）
360 安全卫士团队版
360 Win7盾甲主机安全加固系统
360 终端应用安全访问控制系统
通软终端安全系统V6.5
通软网络接入控制系统V6.5
360 终端安全防护系统(信创版) 信创非密
360 终端安全接入系统(信创版) 信创非密
360 主机监控与审计系统(信创版) 信创非密
360 防病毒系统(涉密专用计算平台网络版) 信创涉密
通软服务器审计系统（涉密专用计算平台版）信创涉密
通软主机监控与审计系统(涉密专用计算平台版) 信创涉密
360 安全浏览器（企业版）
360 安全浏览器（信创单机版） 信创非密
360 安全浏览器（SaaS版）

流量检测与响应基础设施

360 全流量威胁分析系统
360 高级持续性威胁预警系统
360 文件威胁分析系统
360 安全防火墙系统
360 WEB应用防火墙系统
360 网络入侵防御系统

态势感知基础设施

360 态势感知一体机
360 安全分析响应平台

DNS检测与响应基础设施

360 DNS威胁分析平台
360 DNS安全解析系统

网络空间测绘基础设施

360 资产威胁与漏洞管理系统
360 网络空间测绘系统

威胁情报基础设施

360 威胁情报平台
360 威胁态势监控系统

03 专家运营基础设施群

人才培养基础设施

360 安全教育云平台
360 工业互联网安全教育实训平台
360 安全教育实训平台
360 网络安全评估认证考核平台
360 网络安全评估认证模拟平台
360 网络安全评估认证实训平台

应急响应基础设施

360 应急响应中心

安全运营基础设施

360 安全运营中心

安全开发基础设施

360 应急响应中心

04 资源面管控基础设施群

零信任基础设施

360 SDP安全访问平台

密码/证书基础设施

360 SSL电子证书

05 安全大数据平台

安全大数据平台

360 数据资产管理平台

06 其他

其他

360 云安全防护系统
360 云安全检测系统
360 云安全管理平台
360 车联网安全检测平台
360 车联网安全监测平台
360 公有云SaaS云盘
360 私有化企业云盘
360 IM即时通讯
360 奇麟大数据平台
360 评估保
360 加固保
360 移动应用安全合规检测工具箱
360 视频服务平台
360 PaaS服务平台
360 物联网平台
360 机器学习平台
360 云计算管理平台

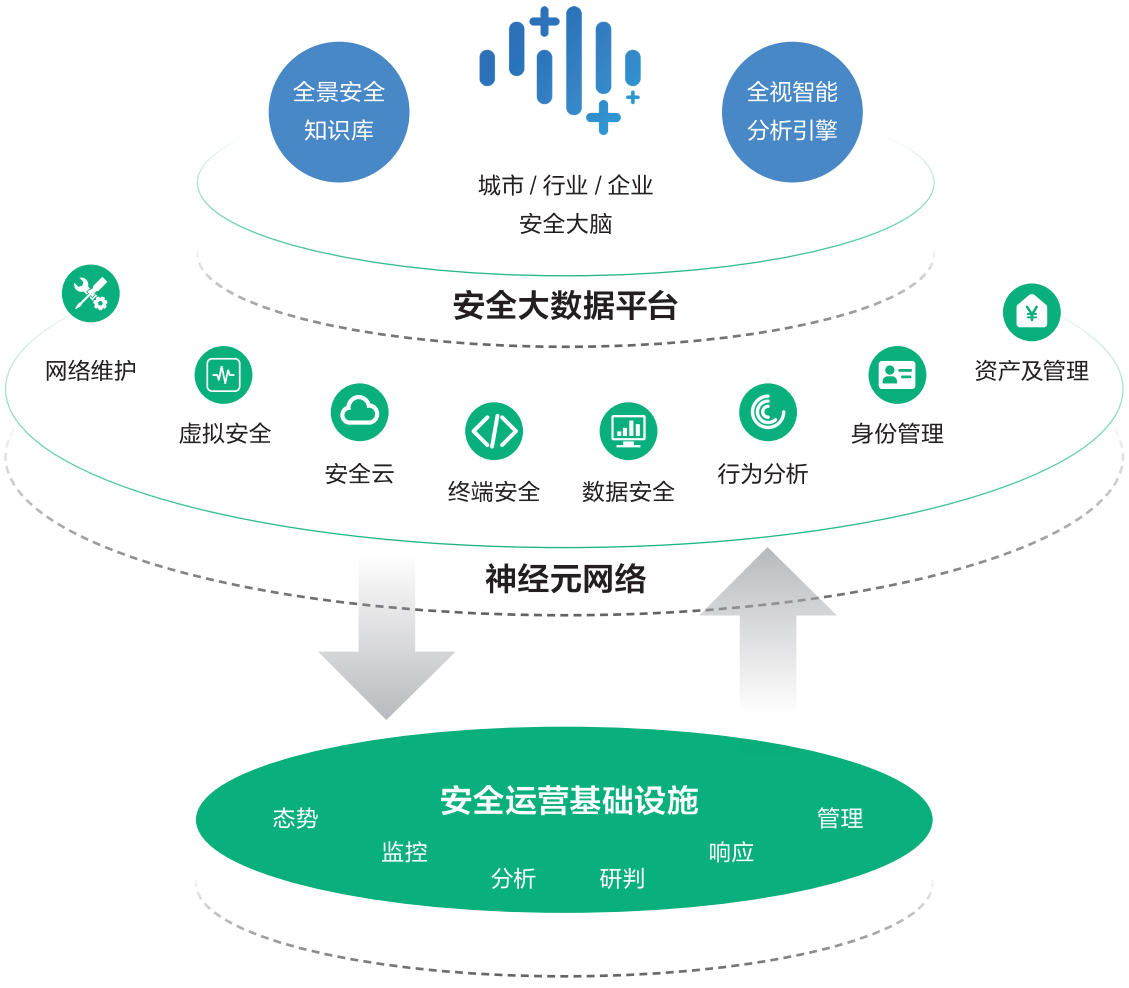
5.3 | 重点安全产品 |

360本地安全大脑

1.产品概述

360本地安全大脑是基于云计算、大数据、人工智能等新一代信息技术，将360云端安全大脑核心能力本地化部署的一套开放式智能分析、研判、预警、响应、评估的统一安全平台，模块化组合形成多场景方案，可视化、自动化、智能化高效完成态势感知、高级威胁检测、威胁自动化响应、抗攻击能力评估等安全工作。

本地安全大脑接受360云端安全大脑和360核心安全大脑赋能、连接安全设备、汇聚安全数据、积累安全知识，帮助客户实现全景安全知识融合，全栈核心技术融合、全视安全大数据融合，全方位提升安全体系能力。



2.技术优势

● 安全大脑赋能

360安全大数据汇集了300亿恶意样本、22万亿安全日志、80亿域名信息、2EB以上的安全大数据，依靠于顶尖安全专家的分析研究，大数据产出的安全知识和威胁图谱从云端安全大脑赋能本地安全大脑，结合本地安全大脑多种威胁分析引擎发现很多传统手段无法发现的安全问题。

● 多维神经元、全视角分析

多维神经元矩阵是360在长期的攻防演练中训练出一整套专业的感知器网络，能够将威胁攻击方方面面的蛛丝马迹都汇聚到本地安全大脑平台上，使得安全人员可以全方位、全视角分析和处置恶意攻击。

● 专家经验指导自动化响应

360安全专家根据多年实战化攻防经验总结出各类型安全运营战法，预置在SOAR系统中固化为可执行的响应预案。客户也可根据实际情况对SOAR中预案进行调整配置，进行快速的威胁检测、安全分析、事件处置等安全运营流程的自动化执行，提升安全运营效率和效果。

● 多阶段降噪、精准化告警

本地安全大脑分析模块多阶段把控告警生成的全过程，通过自循环、自学习逐步提高告警精准度。在安全运营的过程中，不断优化改进数据处置流程、事件分析规则和聚合模型，利用正向循环反馈持续提升告警精准度。

● 整体协防、全局联动

360 由覆盖全球的网络神经元实时监控全网攻击，安全专家持续跟踪分析攻击团队和新型攻击事件，产出威胁情报和检测规则，并下发到本地安全大脑，一旦发现有新型恶意攻击，可瞬时部署到各个端点，实现全局联运整体防御。

● 自动化模拟、实战化评估

AES也就是入侵者模拟攻击技术，基于实战攻防全景知识库，以ATT&CK 攻击技术框架系统化评估安全防御能力，以实战化模拟攻击手段促进系统防护和安全建设。AES提供了边界、内网、邮件、终端、数据防护等多方位评估方案，用户可根据需求自由选择。在设置好攻击代理和靶标后，AES可定期自动执行，结合云端同步，以最新攻击手段自动化评估检验客户的实际防护水平，最后生成分析报告和加固建议，供安全团队改进系统。

● 超级分布引擎、100万EPS超大数据量分析

本地安全大脑数据分析采用先进的数据分析引擎，不但可以支持多数据源、多维度关联分析，还可采用多层级分布式计算方式以支持超大数据量的分析计算，计算规模可达到 100万EPS，即每秒可处理100万笔日志的分析；

● 专家服务、协同防御

360依托于业内顶尖的安全专家，可协助客户进行安全事件的分析、研判、处置等工作，降低客户安全团队在技术、经验上的风险，提升安全运营的效率和效果。

● 多级部署、全局分析

本地安全大脑基于大数据技术实现对海量数据的分析和处置，可根据客户的需求实现总部对下属分部的多级部署，真正实现分级部署、数据同步、全局统一分析；

360终端安全检测与响应系统（EDR）

1.产品概述

360终端安全检测与响应系统（EDR）基于360云端安全大脑和360核心安全大脑安全大数据赋能，依靠多维度高质量的威胁情报、多维度全景安全知识库以及360安全专家团队的支撑力量，能够对高级威胁风险进行深度检测，补充了传统终端安全产品防御高级威胁能力的不足，降低高级威胁最终达到目的可能性，从而实现高效防御效果。

2.技术优势

● 海量安全大数据

安全大数据是360EDR的持续驱动力，基于17年实战经验，360已经汇集300亿恶意样本、2EB 以上的安全大数据，可瞬间调用超过百万颗CPU参与计算、检索和关联多维度威胁数据。基于巨量终端、多年实战所获得的海量安全大数据赋能，360EDR可以有效追溯攻击过程并定位攻击源，帮助政企用户构建终端安全的核心能力。

● 高质量终端数据采集

数据采集质量直接影响EDR的真正检测效果。相较于传统EDR通过应用层HOOK、利用微软ETW的数据采集方式，360EDR还可以通过系统深层次RPC状态追踪、独一无二的核晶硬件虚拟化引擎，记录更完整更精准的参数信息，有效规避噪声数据多、数据精度低、被攻击者绕过等问题，一举克服高质量数据采集难题。

● EDR专业支撑团队

人的因素在终端安全对抗过程中占据重要作用。360安全专家具备真正的从全网实战中总结出来的知识库和安全分析能力，目前已成功挖掘谷歌、微软、苹果等主流厂商CVE漏洞2000个，包揽三巨头史上最高漏洞奖励，并已成功追踪溯源海莲花、摩诃草、美人鱼、蔓灵花、蓝宝菇等针对中国的境外APT组织累计多达50个。依托安全专家的全网攻防经验，360EDR在检测、分析、调查和响应等方面的能力指标得到全面提升。

360终端安全管理系统

1.产品概述

360 终端安全管理系统是在360云端安全大脑和360核心安全大脑的极智赋能下，以大数据、云计算、人工智能等新技术为支撑，以可靠服务为保障，集防病毒、漏洞与补丁管理、Win7盾甲、终端管控、桌面优化、软件管家、安全U盘及移动存储管理等功能于一体的企业级安全产品，同时支持与360终端安全检测与响应系统（EDR）进行集成，帮助政企用户快速构建终端威胁对抗体系，有效保障全网终端安全。

2.技术优势

● 安全大数据

安全大数据是看见威胁的基础，360拥有超过300亿的恶意样本数，且每天以900万的速度增长，涵盖个人用户、政企用户恶意样本，凭借全球前三、东半球第一的安全大数据规模，360终端安全管理系统能够实现恶意样本的全面检出。

● 多维检测引擎

360终端安全管理系统提供云查引擎和本地引擎结合的方式，产品通过云引擎、鲲鹏大数据引擎、QVM Ⅱ人工智能引擎、QEX脚本引擎打造云-地一体的多引擎检测框架，广泛覆盖PE、非PE类样本。QVM作为业界首个采用机器学习技术的反病毒引擎，无需频繁升级特征库即可对包括勒索病毒在内的新型病毒实现高效检出。

● 漏洞挖掘修复

依托360安全专家团队的技术优势，结合360安全大脑的漏洞情报大数据，360目前已经发现超过2000个CVE漏洞。同时，360能针对高危漏洞提供紧急微补丁修复能力，对包括Windows XP、Windows7、Windows Server2003、Windows Server2008在内的停服系统继续提供安全保障。

● 可扩展集成360终端安全检测与响应系统（EDR）

支持与360终端安全检测与响应系统（EDR）进行集成，对文件、进程、注册表、系统、网络等行为进行高精度数据采集，结合360庞大的IOC情报库，对流行APT行为特征和环境特征进行全面检测并定点清除威胁，赋予终端全面有效的APT对抗能力。

● 灵活易用的桌面小助手

360终端安全管理系统提供弹窗防护、文档卫士、启动项优化加速、系统垃圾清理以及文件粉碎机等桌面小工具，帮助终端用户自助管理计算机，提升系统安全运行效率。

360高级持续性威胁预警系统（NDR）

1.产品概述

360高级持续性威胁预警系统，是360自主研发对各类型网络攻击行为（尤其是新型/未知威胁行为、APT组织活跃行为）进行检测、分析、响应的软硬件一体机产品。该系统在360云端安全大脑和360核心安全大脑的赋能下，通过流量深度分析结合全球威胁情报、攻击行为分析、机器学习、关联分析等新一代安全技术，且系统部署简单，攻击发现分析能力突出，在实网攻防演练、重保活动、关键信息基础设施保护等强对抗场景中广泛应用，为用户提供传统IDS等威胁管理产品无法实现的更强保障能力。

2.技术优势

● 云端赋能、本地联动

云端支持360云端安全大脑（安全大数据、全球威胁情报、漏洞情报等）的持续赋能，全球最新威胁尽在掌握；本地支持与终端安全、防火墙、态势感知等联防联动，事件发现响应效率有效提升。

● 业界领先的攻击检测体系

以ATT&CK技战术和知识图谱体系为基础，结合特征检测、威胁情报、行为分析、AI算法等多引擎检测技术实现对各类攻击行为的覆盖，APT组织活跃行为及未知威胁检测能力国内领先。

● 攻击告警自动确认

支持全量攻击告警的自动分析确认，对每条告警结果进行是否成功的分析和标注，同时对每条告警的攻击特征进行自动化高亮展示，不仅有效提升安全告警准度、降低误报率，还可以提升分析优先级和易用性。

● 多场景化的专项分析

对复杂攻击场景通过专题式分析，形成对邮件攻击场景、弱口令攻击、木马异常通信等数十类场景的深度分析输出，并支持时间线、KillChain等可视化分析模型，对相关异常/威胁事件做关联性分析和确认。

● 一体化设备、易于部署

集检测、分析、响应、态势监测模块于一体的ALL-IN-ONE设备，简单部署，易于使用。支持单设备部署，多设备+管控中心的多设备分布或集群部署模式。

360网络攻防靶场平台

1.产品概述

360网络攻防靶场平台是对实网靶场的有效补充与拓展，在360云端安全大脑的极智赋能下，通过构造与现实网络系统相对应的场景模型，结合云平台、虚拟化、攻防技术等手段，打造现实网络系统的平行仿真系统，为现实网络提供“试错”空间，用于学习与培训、测试与验证、评估与演练。

2.技术优势

● 架构前沿

模块化设计，灵活构建各类应用；级联设计，灵活扩展各种规模。 同时分布于本地/异地的多个靶场节点级联可组成大规模联合演训靶场，达到扩展规模、扩充容量、联合调度等目的。

● 内容丰富

资源种类多样，资源内容丰富。平台提供包括靶标库、场景库、工具库、漏洞库、评估规则库在内的各种资源，有效支撑用户各种业务场景应用。

● 技术创新

平台采用私有云抽象、物理设备抽象、态势引擎、全维数据采集等创新技术。这些关键技术来自于360丰富的网络攻防实训、竞赛系列产品，以及多年以来成功举办XCTF国际网络安全技术对抗赛积淀的技术和经验。

360资产威胁与漏洞管理系统（天相）

1.产品概述

360资产威胁与漏洞管理系统【简称：天相】，是基于安全运营、应急响应需求场景开发的常态化资产威胁管理系统。通过运用资产威胁情报以及先进的资产威胁探测引擎，全面识别、管理组织IT边界，确定资产属性、快速发现安全漏洞、精准定位安全风险。通过专业安全加固建议和风险复测，助力组织实现资产安全自主掌控。天相通过对组织IT资产信息的长期管控，帮助组织完善安全资产管理制度，有效应对业务发展引起的资产变更及其带来的安全风险。

2.技术优势

● 建立安全资产管理体系

天相除具备发现企业开放在内外网上的IP、URL等多种数字资产外，还具备内外网资产关联、资产动态持续监测、多维IT资产检索定位、不同管理角色权限定义等结构化的安全管理方式。

● 海量指纹库积累

指纹库是准确识别安全资产版本类型的核心能力，天相指纹库融合开源指纹库、商业指纹库、行业指纹库在内的多源指纹信息。通过数据清洗、融合，已形成5大类、17小类，涵盖操作系统、应用服务、中间件与数据库、工控与物联网设备、区块链协议与服务、虚拟化设备、安防办公设备以及部分金融行业特色业务系统指纹。不记版本号的指纹库条目数量在24000项以上，计入版本信息可达50万条以上。

● 漏洞全生命周期管理

天相通过周期性漏洞监测，持续跟踪漏洞修复和加固状态，通过提供漏洞对应责任人的指派流程，帮助用户掌握漏洞的生命周期变化情况，能够直观展示监测结果和流程结果的比对情况，有效识别新增和重现（未修复成功）的漏洞。

● 无介入式安全检测能力

天相采取黑盒检测（网络可达即可检测）+被动情报碰撞的方式，实现资产威胁监测能力。不对目标资产进行任何安装agent、植入脚本等深度敏感操作，对目标系统影响较低，检测安全性较高。

● 快速响应1day应急

通过长期资产监控维护资产列表，当出现1day的时候，天相能够快速推送相关情报，并根据1day系统/设备/应用版本信息快速定位到可能受到影响的资产，帮助用户排查并修复1day漏洞。

● 资产发现深度广度相结合

在深度上，天相可对目标端口进行深度探测，通过获取指纹信息和banner信息识别真实组件小版本。系统内置的指纹库可支持38大类指纹信息，能全面识别系统应用组件信息。自定义检测范围涵盖全IP段资产至单个IP端口，可灵活定义资产发现任务的检测范围。在广度上，支持内外网域名、IP、端口、url、应用组件、web组件等资产发现能力。天相的内外网全局资产发现能力，对标重保时期的内外网资产暴露监测需求，可满足用户在护网行动等特殊时代的资产威胁暴露监测场景。

● 全面的数据能力支撑

天相具备众多数据能力，可有效支撑组织数字资产威胁监管能力，包括：全球域名库数据、全国备案库数据、全球IP地理信息库数据、漏洞POC库数据。

● 全量API数据赋能

支持基于API的数据输出，可对接360本地安全大脑，为其提供全面、准确、及时的IT资产信息。

360网络空间测绘系统 (QUAKE)

1.产品概述

360网络空间测绘系统——Quake是360网络安全响应中心 (360-CERT) 自主设计研发的一套针对网络空间实体进行自动化探测的分布式系统。作为360云端安全大脑测绘云的核心系统，Quake能够对全球IPv4、IPv6地址进行持续性探测，实时感知全球网络空间中各类资产并洞见其中的安全风险。Quake采用自研的Vscan测绘引擎，实现动态网络资产数据获取，对360安全大脑的知识和线索进行的补充；另一方面，结合360云端安全大脑的海量数据进行关联分析和建模，最终汇聚并呈现出多维度、多视角的网络空间样貌，帮助用户探索网络空间黑暗森林，成为连接现实世界与网络空间的桥梁。

2.技术优势

● 灵活部署并获取能力

提供标准的SaaS帐号服务，快速得到您关注对象的全球分布态势；提供全本地化部署方式，免除特殊安全需求顾虑；大批量元数据订阅和转接，帮助用户赋能现有安全体系；

● 测绘数据积累全球领先

Quake累计测绘全网数据数十亿条，覆盖常见网络协议、工控协议1000余种，包括通信，工控、区块链、IOT、视频在内的16个大类，120个小类，测绘数据积累全球领先；

● 自研Vscan扫描引擎

Vscan扫描引擎能够获取更全面更深入的资产信息，结合人工智能算法模型显著提升识别率，并配合多种任务策略与计算基础设施组合，实现全网动态资产测绘；

● 网络空间虚实映射

利用360数据资源及独有的网络空间测绘技术，针对网络空间中的IP归属与定位进行专项测绘，实现虚拟空间与现实世界的全息映射；

● 360安全大数据赋能

Quake融合2EB安全大数据，包括威胁情报、PDNS、Whois、ICP、证书等，建立多维度多层次网络空间资产视角；

360车联网安全检测平台

1.产品概述

360车联网安全检测平台是一套为智能网联汽车提供网络安全验证的基础设施。平台通过完善的测试管理流程，将安全检测工具/引擎和检测知识库进行场景化融合，结合360云端安全大脑威胁情报数据，为车企、汽车检测机构的汽车网络安全合规检测、安全验证等场景提供安全验证环境，有效保障智能汽车安全入网工作开展。

2.技术优势

● 集成多种智能网联汽车专用安全检测工具

360车联网安全检测平台集成了多种自研的智能网联汽车安全检测工具引擎，能够对车载网关、T-BOX、车机的系统、通信、无线等组件进行安全测试，有效支撑智能网联汽车云-管-端各层级的安全检测工作开展。

● 丰富的检测知识库

360 Sky-Go安全团队拥有多年的智能网联汽车安全研究、渗透测试经验，实战案例覆盖80%车企、100多个车型，为360云端安全大脑形成了丰富的智能网联汽车安全检测知识库，为安全验证、攻击测试、漏洞验证提供了简易可行的验证方法。检测知识库可支撑的安全检测业务包括：合规性检测、安全设计符合性检测、安全审计、渗透测试等，覆盖攻击面包括车载各类零部件及服务系统，例如：IVI、T-BOX、GW、域控制器、ECU、OTA、TSP、APP、无线网络、车载网络等。

● 完整的测试管理流程

360车联网安全检测平台提供了完整的测试管理流程，能够全程跟踪车型安全测试的过程，对测试资产、测试物料、测试用例、测试任务、测试结果、漏洞、报告进行统一的管理，通过不同角色的任务流转机制，协调并保障测试工作在车企、供应商、安全测试团队的快速推进。

● 灵活的扩展能力

360车联网安全检测平台具备强大的扩展能力，可集成第三方检测工具，将测试结果整合到车型项目报告中，便于用户的统一管理。

360 车联网安全监测平台

1.产品概述

360 车联网安全监测平台基于对车联网环境的重要组件（如：IVI、T-Box、OBU、RSU 等）的数据采集，利用大数据分析等先进技术，结合360云端安全大脑提供的分析预警和威胁情报，为车企、车路协同示范区车联网系统建立安全威胁感知分析体系，实现智能网联汽车安全事件的可感、可视、可追踪。该平台符合智能网联汽车合规准入，以及ISO/SAE 21434、ITU-T X.1376 标准的相关要求。

2.技术优势

● 全面的车联网安全事件感知

平台可对智能网联汽车进行持续监测，通过部署在车载零部件中的神经元，分析并发现车辆网络攻击事件及异常行为，为汽车的网络安全监控提供有力手段，保护在路车辆的安全行驶。

● 专业的车载监测及响应神经元

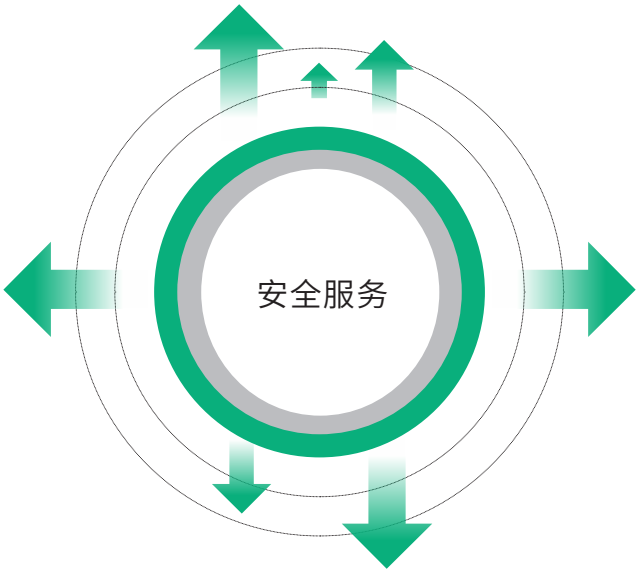
车载入侵检测与防御系统（IDPS）部署于车载控制器的MPU 或MCU 中，为平台安全事件分析与处置提供端侧能力支撑，系统支持插件化，安全策略云端编排、灵活调度，支持Android、Linux 系统，NXP、MTK、高通等硬件平台，满足主流车载控制器的部署要求。

● 丰富的车联网安全事件分析策略

平台基于Sky-Go 团队多年车联网漏洞挖掘、安全研究、渗透测试经验，形成了丰富的知识库，可有效识别车联网安全事件及异常行为。

5.4 | 安全服务 | SECURITY SERVICE

安全运营服务
专项评估服务
威胁分析服务
红蓝对抗服务
安全众测服务
安全运维服务
重大时期安全保障服务
风险评估服务
渗透测试服务



应急响应服务
等保咨询服务
安全培训服务
安全意识演练服务
应急演练服务
数据安全服务
代码审计服务
云安全服务
移动安全服务

360安全专家服务

	评估、改进	检测、分析	响应、止损	恢复、复盘	
体系专家 基于核心资源的VIP服务	安全体系规划 数据防护咨询 信创规划咨询 漏洞管理咨询	APT发现追踪 APT攻击分析 零日漏洞和攻击套件发现	APT攻击溯源		高级安全托管服务 (MDR)
	入侵者模拟-防护评估 入侵者模拟-防护改进 入侵者模拟-预警验证	全视监测预警 全视安全分析 全视威胁狩猎	全视事件验伤 全视调查取证 全视应急响应 全视溯源分析	全视共生情报 全视情报赋能	
	高保真实战靶场管理 高保真实训靶场管理				
领域专家 基于专业和经验的研判服务	安全场景建设 安全合规规划 安全开发咨询 合规场景建设			数据恢复 网站修复 网络修复 系统修复	安全托管服务 (MSS)
	安全培训 人才认证				
	渗透测试 红蓝对抗 漏洞众测				
一线专家 基于标准化流程的护理服务	合规预评估 代码审计 脆弱性扫描 系统加固 安全配置运维	安全大脑装配调试 神经元接入 数据盘点 资产盘点 安全报告			
		网站监测服务 仿冒网站鉴别 产品职守 安全巡检 网站职守			

新一代MSS托管安全服务

1.产品概述

新一代MSS托管安全服务是360集多年政企客户安全建设和服务经验，面向客户侧数字化场景和新一代安全运营的需求，以提升实战化安全能力为导向，以安全结果可管可控为目标，全新推出的一站式托管安全服务，结合360掌握的全网安全态势、安全实战方法论和丰富的实战经验，助力政企客户安全能力与运营效率的持续提升。

2.技术优势

● 体系化的运营理念

结合360拥有的全球最大的样本库、攻防知识库、安全大数据以及业界先进安全理念形成的安全运营知识图谱，帮助客户构建贴合业务发展的网络安全运营体系。

● 实战导向安全能力

作为安全实战方法论的创立者，360倡导以攻防实战提升安全能力，依托多年积累的基于实战的攻防战法、技术、程序和大量独有知识库，帮助客户积累有效应对风险的安全能力。

● 顶级安全专家团队

专业的安全分析师资源以及运营团队扎实的专业化技能和丰富的实战经验，具备诸多国际认可高级资质，能够为客户提供专家级高质量的安全运营服务。

● 成功案例经验借鉴

360已经落地了包含城市级、行业级、企业级的诸多安全运营案例，具备成熟安全运营方案、实施计划、运营团队，通过运营经验的互通共享全力保障客户的业务发展。

5.5 | 解决方案 | SOLUTION

● 政府行业

政府行业信创跨平台安全办公解决方案
政务云安全解决方案
实训竞赛解决方案
网络攻击欺骗解决方案
网络安全科普基地建设方案
网络安全意识服务方案
网络安全合规培训方案
网络安全组织能力提升方案

● 央企行业

安全运营中心解决方案
企业网络安全意识服务方案
网络安全人才岗位能力提升方案

● 公检法行业

公安行业信创跨平台安全办公解决方案
零信任安全访问解决方案
网络靶场解决方案
实训竞赛解决方案
网络攻击欺骗解决方案
公安行业网络安全解决方案

● 金融行业

金融行业信创过渡期应用兼容安全解决方案
零信任安全访问解决方案
网络靶场解决方案
实训竞赛解决方案
网络攻击欺骗解决方案
安全评估测试解决方案
反欺诈解决方案
一站式安全防御服务解决方案
金融科技网络安全意识服务方案
数据安全人才培养方案
金融机构网络安全人才岗位能力提升方案

● 烟草行业

云安全访问和管理解决方案
实训竞赛解决方案
网络攻击欺骗解决方案
企业网络安全意识服务方案
网络安全人才岗位能力提升方案

● 军队行业

信任评估与动态授权管理解决方案
网络靶场解决方案
实训竞赛解决方案
网络攻击欺骗解决方案
军队行业网络安全解决方案
实战技术人员队伍培养方案

● 交通行业

车联网网络安全监测运营解决方案
车联网网络安全合规检测解决方案
等保合规安全解决方案
实训竞赛解决方案
网络攻击欺骗解决方案
轨道交通行业安全解决方案

● 财政行业

零信任内网安全解决方案
网络攻击欺骗解决方案

● 运营商行业

攻防演练解决方案
终端安全管理解决方案
360应龙综合反诈防骚扰平台
云安全资源池解决方案
网络靶场解决方案
实训竞赛解决方案
网络攻击欺骗解决方案
网络安全人才岗位能力提升方案
网络安全意识服务方案

● 智能制造行业

智能制造行业安全解决方案
智能制造安全实验室建设方案
智能制造网络安全意识服务方案
工业互联网网络安全人才岗位能力提升方案

● 电力行业

国家电网终端安全解决方案
发电厂电力监控系统网络安全解决方案
智能变电站网络安全建设方案
电力行业信创过渡期应用兼容安全解决方案
零信任内网安全解决方案
网络靶场解决方案
实训竞赛解决方案
网络攻击欺骗解决方案
电力行业网络安全意识服务方案
网络安全人才岗位能力提升方案

● 石油化工行业

石油石化网络安全解决方案
企业网络安全意识服务方案
网络安全人才岗位能力提升方案

● 轨道交通行业

企业网络安全意识服务方案
网络安全人才岗位能力提升方案

● 公安行业

网安技术人员队伍建设方案
科信技术人员队伍建设方案

● 教育行业

▪ 产业学院

360现代产业学院服务方案

▪ 政策性服务

教育部协同育人项目服务方案
供需对接就业育人项目服务方案
1+X职业技能等级认证服务方案
网络安全三教改革服务方案

▪ 专业建设

网络安全专业建设服务方案
网络安全人才培养服务方案
网络安全课程教材服务方案
网络安全师资培训与服务方案
网络安全实习实训服务方案
网络安全技能竞赛服务方案
网络安全课证融通服务方案

▪ 实验室建设

网络安全攻防实验室建设方案
数字安全实验室建设方案
工控安全实验室建设方案
工业互联网安全实验室建设方案

▪ 产教融合

网络安全产教融合实训基地建设方案
网络安全科普基地建设方案
网络安全教学体验中心建设方案

360

THE LEADER IN DIGITAL SECURITY

360
GOVERNMENT
AND ENTERPRISE
SECURITY
GROUP

360

THE LEADER IN DIGITAL SECURITY

06

创新技术落地及实践

① 6.1 信创技术相关落地及实践
② 6.2 重点产品相关落地及实践
③ 6.3 护航国家重大政治安保活动实践
④ 6.4 360城市安全大脑实践

360
GOVERNMENT
AND ENTERPRISE
SECURITY
GROUP

6.1 | 信创技术相关落地及实践 LANDING & PRACTICE

360赋能信创安全能力体系建设

2005 积累期

将360多年积累的安全大数据知识库、实战攻防样本库、安全检测分析能力、威胁情报和专家服务等赋能信创领域。

2018 发展期

360安全浏览器和360终端安全防护系统率先布局信创领域，适配主流国产计算平台，保障信创终端安全办公；发布国密根证书计划，推进信创领域国密算法落地。

2020 深化期

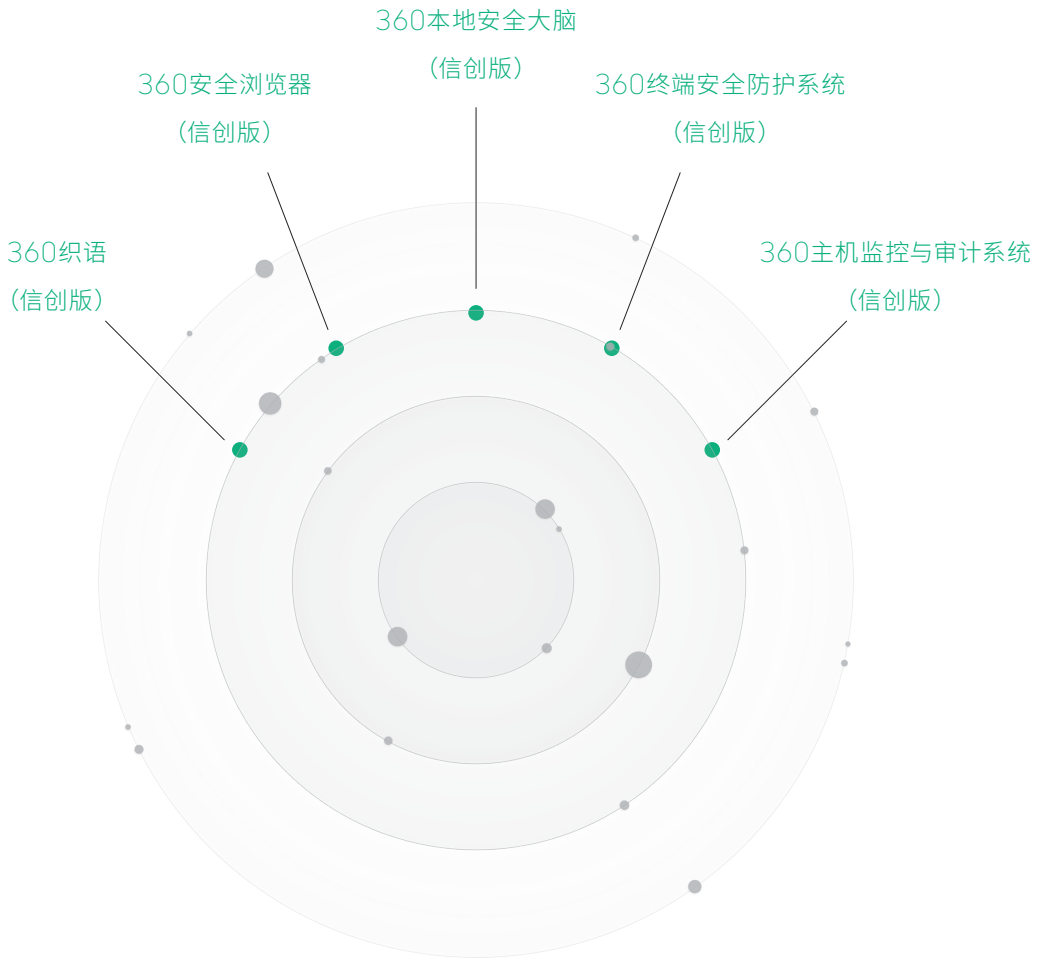
继续发挥核心优势输出安全能力，将360本地安全大脑信创解决方案成功应用于天津信创安全基地、上海市徐汇区服务中心、陕西省司法厅、四川信创中心等安全运营项目中，携手生态伙伴推动我国信创产业高速发展，覆盖党、政、军、企全行业。

360已适配的信创生态

国产芯片	飞腾	龙芯	兆芯	申威	鲲鹏
操作系统	统信	红旗	普华	鸿蒙	
	银河麒麟	中标麒麟	华为云桌面	中科方德	

360信创安全产品

360政企安全集团基于17年实战经验打造了信创安全大脑体系，其中360本地信创安全大脑是信创安全体系建设的重要安全管理产品，主要包括四大能力平台：大数据处理平台、检测分析平台、安全运营平台和应急响应平台，此外，在360云端安全大脑赋能之下，360终端安全防护系统、360主机监控与审计系统、360安全浏览器、360织语等信创产品全方位守护政企用户信创终端安全、业务安全、数据安全等，同时为用户提供了安全的跨平台兼容体验，大幅降低了信创迁移的落地成本。



信创产品

360安全浏览器V10

1.产品概述

360安全浏览器具有内核安全可控、启动速度快、网页渲染能力佳等特点，采用领先的国密套件支持，完整的信创迁移方案，为政企客户提供最极速、最安全、最易用的浏览器。全面支持信创主流CPU、操作系统、流版签办公插件、国密单双向通信加密、国密根证书管理、USBKEY驱动管理、显卡硬件加速（AMD系列）、用户隐私数据保护等，高效满足信创平台办公需求，打造信创平台Web应用统一支撑平台，建立基于浏览器的Web生态标准体系。

2.产品优势

▶ 信创生态建设

兼容信创目录主流国产芯片(飞腾、鲲鹏、麒麟、龙芯、龙芯Arch、兆芯、海光)和操作系统(UOS、银河麒麟)，同时支持国内主流行业专用操作系统；152份产品兼容互认证书，共同建设信创最佳办公一体化平台。

▶ 安全可信防护

采用严格的“非白即黑”安全防护策略，有效防止网站追踪和数据泄露行为，阻断危险脚本执行，有效拦截非法可疑网站，结合安全的DNS服务，提高浏览网络时的安全性和隐私性，为用户提供全方位立体保护。

▶ 自有根证书库

全球第五大、中国第一大自有根证书库：覆盖98%HTTPS流量，确保网站真实可信。360建立国内唯一自有国密根证书库，目前已有20家CA的65个根证书加入360根证书计划，完善的浏览器国密根证书信任机制，对网络防泄密、抗侵入、识真伪、保安全起到重要作用。

▶ 信创迁移方案

顶级浏览器专家服务，通过360扁鹊检测及修复、NP/PP插件支持和UA切换、视频解码及硬件加速、统一控制等一系列信创迁移解决方案，全面指导客户从Windows平台平滑迁移到信创平台，让业务系统不仅在信创平台可用，并且达到好用。

▶ 商用密码模块

内置浏览器密码模块，支持SM2/SM3/SM4国密算法，符合《信息安全技术—传输层密码协议(TLCP)》、《SSL VPN技术规范》、《密码模块安全技术要求》标准，支持国密根证书管理、国密双向认证KEY驱动管理、双证书自动协商、国密网关联动等，形成自有完整的国密改造解决方案。

360终端安全防护系统

1.产品概述

360终端安全防护系统（信创版）是在360安全大脑的极智赋能下，以大数据、云计算、人工智能等新技术为支撑，面向政府、军队、军工等企事业单位推出的以安全防御为核心、以安全策略管控为重点、以自动化运维管理为支撑的专业国产主机防护产品，可针对国产操作系统实现病毒木马查杀、终端管控、安全审计等功能，有效遏制内外部威胁的传播与扩散途径，保障内网终端主机的安全，全方位提升核心业务及资源的安全性。

2.五大反病毒引擎

▶ 云查杀引擎：

10万+服务器，EB级存储，样本数量超过300亿，多线路云查绿色通道，每天响应超700亿次。

数据最全/范围最广/响应最快的云查引擎

▶ 360 KP引擎：

有效识别全球80亿+ 病毒文件，业界最轻特征引擎，病毒库的广谱率1：10000。

有效识别全球83.2亿各类恶意程序

▶ EAV引擎：

Linux/国产化终端专用查杀引擎，精准检测与识别ELF文件病毒。

广谱查杀/逻辑控制/感染型修复能力

▶ 360 QVM II：

EB级训练样本，十年模型优化，引擎检出率超长半衰期，有效增强离线查杀能力。

支持向量机技术的杀毒引擎

▶ QEX引擎：

精准识别可执行脚本、安装脚本、宏等恶意脚本对office 有效清理宏病毒，还原珍贵文档。

高效识别脚本病毒，提升检测效率

3.核心优势

▶ 强大的适配能力，全面兼容国产操作系统

可全面兼容中标麒麟、银河麒麟等主流国产操作系统，并可完美运行于龙芯、飞腾、兆芯等国产CPU平台之上。针对国产操作系统特性设计了病毒扫描、实时防护、终端管控、等功能，确保不与国产系统中的办公软件产生冲突。

▶ 统一管理平台，实现灵活管理

适配政企单位国产化终端环境，可针对不同分组和终端，制定合适的安全策略，提供可落地的安全方案。

▶ 专用查杀引擎，适配国产化环境

提供专门适用于国产化终端的EAV引擎，覆盖Linux环境流行样本，有效检测ELF文件格式的感染型病毒。

▶ 自主知识产权，杜绝后门隐患

完全自主知识产权，掌握核心技术，杜绝安全后门，能够为国产化终端输出持续可靠的安全防护能力。

360政务应用典型案例

基于信创浏览器的安全办公平台

● 典型客户一核心需求

某检察院面临业务稳定困扰、运行维护复杂、终端安全威胁、业务应用迁移难度大、信创终端技术路线复杂性的挑战，需要360浏览器提供应对上述场景的安全办公解决方案。

● 典型客户二核心需求

某省级政务信息化建设运营公司需求场景：

① 解决国密加密算法通讯，

② 适配国产操作系统及国产应用，

③ 支持证书统一信任管理，

④ 实现跨平台一致性办公体验，

⑤ 保护Web业务数据安全。

● 360安全浏览器信创版

- 提供Web应用建设标准，助力信创应用迁移
- 高版本安全内核，支持NPAPI/PPAPI插件标准
- 支持国密SM2/SM3/SM4算法，预置国内权威国密根证书
- 丰富的国密联调适配经验，便捷的国密配置功能
- 广泛兼容SSL网关、智能密码钥匙、数字证书等密码产品
- 提供基于B/S应用的兼容性检测和修复能力（360扁鹊）
- 提供基于C/S应用的跨平台开发工程框架（360易创）
- 提供专家级浏览器技术排障、咨询和指导服务

● 解决方案

业务稳定：与客户核心垂直业务应用深度融合，提供专属定制、适配调优等服务，解决易用性、兼容性、稳定性、安全性等问题，保障业务稳定性，提升办公效率。

安全威胁：支持国产商密码落地应用，完成密评验收，全面修复浏览器安全漏洞。

降本增效：实现终端零配置，浏览器管理中心统一推送配置策略、大幅降低运维成本。

跨平台兼容：一套代码编译，跨平台运行，支持Windows+信创+Mac全PC终端。

● 客户价值

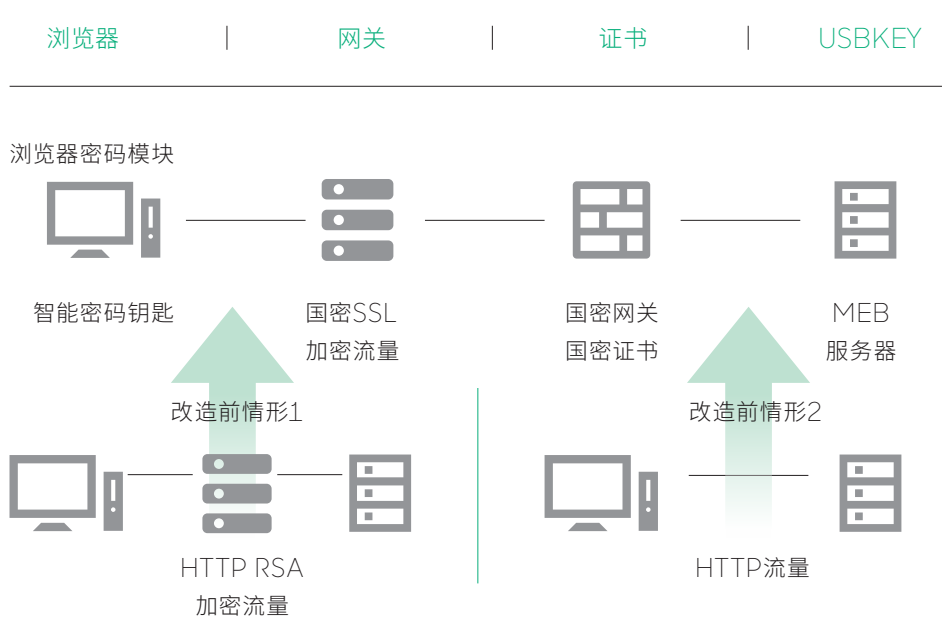
一个平台：统一的浏览器管理中心，Windows/信创跨平台支撑助力国产化替代过渡阶段，保持用户一致性体验，支持SaaS多租户运营模式。

数字资产保障：帮助用户完成国密改造，多维度安全加固功能保障用户核心数字资产。

三个统一：统一Web标准规范、统一应用访问入口、统一管理服务。

密码测评：与政务云深度融合，为政务云提供集约化的密码服务基础设施。

国密改造—链路通讯加密方案



10000+
覆盖政企

100%
行业覆盖

32个
覆盖省级行政区

数百万
覆盖用户

15年
浏览器技术沉淀

NO.1
信创市场渗透率

ONLY 1
全球唯一标准/国密双证书库

1120件
技术专利申请数

83%
信创市场占有率

TOP 1
安全漏洞致谢榜名列前茅

200+
信创兼容互认证书

1ST
首批支持国密算法

天津信创安全基地安全运营建设项目

本项目建设背景和意义

•360中标天津信创安全运营和应急响应中心建成项目，提出新一代数字安全能力框架，满足天津市信创产业发展需求，帮助天津市建立一套能力完备、可运营、可输出的信创安全体系。

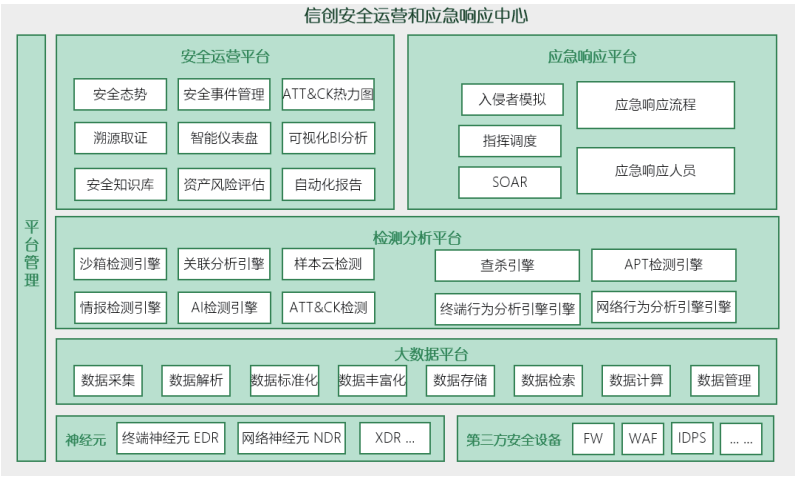
•具体服务内容包括：网络靶场攻防类服务、信创漏洞托管及渗透服务、信创安全应急响应类服务、信创网络安全人才培养类服务。

•360本地安全大脑（信创版）已经成功应用于天津信创安全基地—安全运营与应急响应中心，获评国家工业信息安全发展研究中心"第二届信息技术应用创新安全优秀解决方案"。

01.减低社会使用成本，助力信创产业的持续发展

02.国内首家信创安全基地，为天津信创工程保驾护航

03.加速产业、人才聚集，提升地区信创产业竞争力



本项目建设思路

360政企安全集团以《网络安全法》为指导，在等保制度基础之上率先打造天津信创安全基地，建设一套基地基础设施、一套安全基础设施、一个网络安全靶场、一个漏洞综合管理中心、一个安全运营和应急响应中心、一个安全人才培训中心，以“1+1+1+3”的模式为天津市信创产品供应商和信创用户提供公共服务。

本项目核心价值

•有效降低信创企业在信创安全检测、安全监测以及安全应急响应服务方面的投入。

•为信创产品研发工作提供安全能力和服务保障，使其更专注于创新技术和产品性能研发。

•以“信创+安全服务”模式打造天津信创产业安全新业态，吸引国内信创产业链企业落户中国“信创谷”。

信创生态合作伙伴（排名不分先后）

6.2 | 重点产品相关落地及实践 | LANDING & PRACTICE

360&湘潭大学

打造数字化实战教学体系 赋能教育行业安全建设

“博学笃行，盛德日新”，勇于创新是刻画在湘大人心中的不变信念，更是湘潭大学建校64年以来烙印下的浓重底色。在万物向新的数字化浪潮下，网安人才是破解时代创新的答案。因此，湘潭大学成立了湖南省唯一的网络空间安全学院。学院成立之初，学科方向不凝练、师资力量较薄弱、网络安全实践场景缺乏等难点一一出现。

基于在网安专业实践教学体系、网络空间安全科普基地建设等方面的相同理念，2020年7月，湘潭大学与360政企安全集团不谋而合，正式达成签约合作。自合作开启后，360政企安全集团与湘潭大学合力打造出了基于产出导向的网安实践教学体系。在该体系中，360网络攻防综合靶场成为其中的重要支撑，不仅可以针对性地为湘大学子提供实际的安全项目，还能够在认知实习，专业实习等环节提供多方位的赋能。

湘潭大学计算机学院网络空间安全学院院长李澄清表示：“得益于360政企安全集团的协助，让我们探索出了湘大专属的网安实践教学体系，帮助热爱网络安全的湘大学子能够与国际一流的360安全专家，面对面探讨专业的安全课题；在360网络攻防靶场平台等安全产品中，感受到真实网络空间的攻防博弈”。

湘潭大学计算机学院网络空间安全学院院长李澄清

360&中国广电

安全赋能，开拓电波媒体数字化的新坦途

数字化转型的稳步推进，持续带动着媒体向更深层次融合，以广播电视为代表的电波媒体迎来了颠覆性的变革。但在融媒体时代，伴随传播“茧房”的壁垒被打破、业务规模的增大、业务复杂性的增强，不断为电波媒体提出了更高的安全要求。

为此，中国广电基于科技赋能的战略部署，选择360政企安全集团打造出更全面的安全防护策略。凭借双方合力打造的智慧广电安全运营大脑，中国广电实现了对全国各省网络公司、电视台、融媒体等单位进行安全赋能。

其中，中国广电不仅可以通过本地安全大脑，收集到全国各级融媒体中心和广电分支机构的安全数据，完成实时的监管；借助系统实网攻防平台，对各级单位进行安全可靠性验证；还可通过统一的漏洞管理平台，向各级融媒体中心提供自动化的运维工具，并协助各单位储备应急安全支撑，让中国广电能够时刻保证第一时间的安全发声。

中国广电·青岛5G高新视频应用安全重点实验室总工 党超辉

360&绿城集团

撬动新市场，塑就中国数字房地产的安全标杆

中国房地产行业经历了几十年的发展，已经成为国民经济和金融体系中的重要环节。在数字经济高效发展的当下，数字化技术与地产科技的融合不断加快着整个行业的发展速度，全面撬动崭新的市场格局。但房地产处于数字化的早期阶段，也正在经历着成长的烦恼。如何保证楼盘建设规划、设计参数等关键数据的安全可靠；如何让科技助力公司管控漏洞、病毒等安全风险等一系列挑战，成为国家重点关注的课题。

作为中国领先的优质房产品开发及生活综合服务供应商，绿城集团以优质的产品品质和服务品质引领行业。在中国房地产数字化转型方面，绿城集团走在了行业的前端，不仅组建了专门的信息安全团队，并提出了5年安全建设规划。在此期间，360作为绿城集团的重要合作伙伴，也持续为绿城集团的网络安全建设提供了有力的支撑。绿城集团信息安全工程师陈靖鸿表示，360 EDR产品实现了对集团所有终端和服务器的系统性管控，与各类病毒漏洞查杀等问题，有效提升了云管端解决方案中关于终端安全方面能力。

未来，绿城集团将持续加深与360在终端安全管理、安全运营等多方面的密切合作，打造出中国数字房地产领域的标杆案例。

绿城集团信息安全工程师 陈靖鸿

360&宜兴市工信局

数字政府项目，助力提升数字化安全运营能力

为了动态适应数字政府基础设施环境的变化，充分考虑数字政府基础设施的实时风险，宜兴市工信局对电子政务安全运营服务项目提出了安全运营管理体系建设、建设本地安全大脑运营平台、建设常态化安全运营服务、数据安全体系建设等方面的需求，以达到建设以大数据为基础的本地安全大数据运营平台，构筑本地安全大数据运营平台与云端安全能力的赋能体系，完善安全管理制度流程和安全管理责任边界，实现数据库安全防护、审计等目的。

基于用户多元化需求，360政企安全集团制定了因地制宜的解决方案。该解决方案坚持贯彻“安全运营闭环管理并基于数据分析为核心”的安全运营理念，结合宜兴市信息化基础设施具体情况和现实需求进行设计，形成威胁预测、威胁防护、持续检测、响应处置的闭环安全运营体系。

该项目的落地不仅受到了客户的好评，还被宜兴市工业和信息化局作为典型案例，参与了“2021年江苏省网络安全优秀实践案例”的申报。该项目实现了安全事件的溯源，委办单位业务系统上政务云的申请规范，确保系统上线前后的业务安全，同时还实现了平台化管理不断增加的业务资产，本地专业安全服务团队运营。

6.3 | 护航国家重大政治安保活动实践
SECURITY ACTIVITIES PRACTICE

360已经成为国家网络安全保障的核心力量，在庆祝中国共产党成立100周年大会、两会、十九大、九三阅兵、“一带一路”峰会、G20、金砖会议、上合青岛峰会、进博会、APEC、七十周年庆典、长征5号火箭复飞、北京2022年冬奥会以及支撑国家级网络安全实网攻防演习等重大安保相关工作中发挥了重要作用。

第十三届全国人民代表大会

中国共产党第十九次全国代表大会

北京2022冬奥会

中华人民共和国成立70周年

支持国家级实战靶场攻防演练

6.4 | 360城市安全大脑实践
PROJECT PRACTICE

天津

360城市安全大脑落地天津，为新型智慧城市提供一站式、全场景、全方位的城市安全防护服务。

重庆

360网络安全协同创新产业基地落地重庆，构建西南大安全基地和分布式安全大脑西部节点。

青岛

360中标2.5032亿元的青岛网络安全产业基地相关项目，这是360宣布政企战略后的第三单2亿以上项目。

上海

360政企安全集团成功中标2.1亿元上海市普陀区城市安全大脑项目信息化及配套设施项目，整体提升上海市的数字安全能力。

郑州

360政企安全集团中标2.36亿元国家网络安全产业基地重大基础设施群项目，打造郑州安全大脑。

珠海

360政企安全集团与珠海市人民政府签署战略合作协议：双方将围绕安全城市建设、新型智慧城市开展深度合作。

鹤壁

360政企安全集团与河南鹤壁达成战略合作，成功中标1.1亿元鹤壁网络安全协同创新产业基地项目，共同打造“鹤壁安全大脑”。

苏州

360政企安全集团中标2.608亿元苏州网络安全协同创新暨安全大脑项目。

周口

360政企安全集团成功中标4亿元周口数字城市安全大脑项目，将打造周口数字城市安全大脑，建设安全基础设施赋能数字化场景，为周口市建设中原崛起新高地增添新动能。

360

THE LEADER IN DIGITAL SECURITY

07

ISC互联网安全大会

360
GOVERNMENT
AND ENTERPRISE
SECURITY
GROUP

ISC 2019
第七届互联网安全大会
INTERNET SECURITY CONFERENCE 2019
第七届互联网安全大会
INTERNET SECURITY CONFERENCE 2019

INTERNET SECURITY CONFERENCE

360

THE LEADER IN DIGITAL SECURITY

INTERNET SECURITY CONFERENCE

2013.9.23

(第一届互联网安全大会)

2014.9.24

(第二届互联网安全大会)

2015.9.28

(第三届互联网安全大会)

2016.8.16

(第四届互联网安全大会)

2017.9.12

(第五届互联网安全大会)

2018.9.24

(第六届互联网安全大会)

2019.8.19

(第七届互联网安全大会)

2020.8.5

(第八届互联网安全大会)

2021.7.27

(第九届互联网安全大会)

ISC是中国的互联网安全大会

全球网络安全看中国，中国网络安全看ISC
打造全球性的网络安全发展趋势风向标

于国家：

立足本土拥抱世界，搭建全球网络安全“政产学研用”交流空间，讲述中国网安故事，传递中国声音，致力于实现“全球网络安全看中国，中国网络安全看ISC”发展目标。

于企事业：

整合国际、政府、机构、行业与安全产业多维资源，孵化中国特色网络安全生态联盟，助力网络安全产业精细化、规模化多维发展，践行网络强国思想。

于行业：

展示推介顶尖技术前沿产品，共享全球网安产业创新成果，打造专业性、权威性、全球性的中国网络安全产业名片，加速中国网络安全产业迈向新一代技术制高点。

于从业者：

凝聚全球顶级专家领袖和高端专业人才，组建高端网络安全智库，加强全球网安产业思想碰撞交流，助力网络安全空间共建共治共享共赢格局发展。

十年积淀 夯实行业权威引领新浪潮

亚太地区规格最高、规模最大、影响力最深远的安全峰会

20场 国际峰会	300+场 论坛	30+场 特色活动	2000+ 行业议题
500+位 国际智囊	500+ 厂商入驻	30000+ 每场人次	300+ 产品发布

一席家国梦 引领十年行业新动向

传递前瞻战略声音，助推产业协同发展，探寻网安未来新篇

2013
共筑网络安全世界

2014
互联世界 安全第一

2015
数据驱动安全

首个提出网络安全企业要以大数据能力为基础，形成看见高级威胁的能力。

2016
协同联动·共建安全+命运共同体

2017
万物皆变,人是安全的尺度

2018
安全从0开始

2019
应对网络战 共建大生态 同筑大安全

首个提出网络战观点，网络安全企业需站在国家高度，摒弃行业壁垒，共建网安大生态。

2020
数字孪生时代下的新安全

首个提出数字孪生时代观点，传统安全防护亟需改变，需要网络安全新理念、新框架。

推出网安会议平台
ISC“永不闭幕”

2021
网络安全需要新战法
网络安全需要新框架

首个提出“一个指导、两个融合”的网络安全新战法，倡导以作战、对抗攻防思维为指导，建立应对未知挑战、解决未知问题的安全能力体系。

2022
十年敬请期待

高端网络安全智库

ISC智库齐聚500+各领域智库专家，共商安全趋势

政府领导和顾问专家

邬贺铨
ISC名誉主席
中国工程院院士

王秀军
ISC名誉主席
中国网络空间安全协会
理事长

韩启德
十二届全国政协副主席
中国科协北京大学
科学文化研究院院长

樊友山
全国工商联党组
副书记、副主席
中国民间商会副会长

尚冰
中国互联网协会
理事长

赖明
全国政协副秘书长
九三学社中央委员会
副主席

朱宏任
中国企业联合会、
中国企业家协会常务副会长
原工业和信息化部党组成员

蔡吉人
中国工程院院士

倪光南
中国工程院院士

沈昌祥
中国工程院院士

郭孔晖
中国工程院院士
车联网专家

方滨兴
中国工程院院士
中国电子信息产业集团有限公司
首席科学家

INTERNET SECURITY CONFERENCE

方滨兴
中国工程院院士
国家数字交换系统工程
技术研究中心 (NDSC)
主任

吴建平
中国工程院院士

廖湘科
中国工程院院士

张景安
中国科技体制改革研究会
理事长
国际欧亚科学院
副主席

郭启全
公安部网络安全保卫局
一级巡视员
副局长兼总工程师

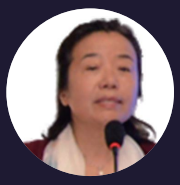
陶青
工业和信息化部
网络安全管理局
副局长

暴 剑
北京市朝阳区区委
常委副区长

景凤启
中国保密协会会长

严明
公安部第一第三研究所
原所长 中国计算机学会
计算机安全专委会荣誉主任

于锐
公安部第一研究所副所长
中国计算机学会
计算机安全专委会主任



冯燕春
国家信息技术安全研究中心
常务副主任

郝叶丽
ISC “观潮” 网络空间论坛
主席

黄胜华
公安部第三研究所
所长

毛作奎
中央网信办
网络安全协调局副局长

张新
工业和信息化部
网络安全管理局
副局长

国际政要、技术专家

I他们曾在ISC分享国际安全政策，探讨国际先进技术

海外大咖

Tom Ridge
“9·11后”美国首任
国土安全部部长、
前宾夕法尼亚州州长

Keith Alexander
美军网络司令部前司令
国家安全局第十六任局长
IronNet Cybersecurity
公司CEO兼总裁

John Allan Davis
前美国陆军少将、
美国Palo Alto Networks
副总裁、首席安全官

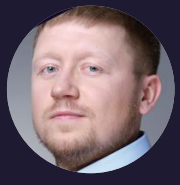
William A. Owens
前美国四星级海军上将
现美国AEA基金
亚洲区主席

John McAfee
McAfee公司创始人

Fred Cohen
计算机病毒之父

Whitfield Diffie
A.M
图灵奖得主

Maor Shwartz
Q-recon公司
漏洞经纪人

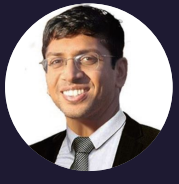


Alexander Liskin
卡巴斯基实验室启发检测
和漏洞研究小组
负责人

Avi Dichter
以色列国会
外交与国防委员会主席

ThomasDullien
著名黑客
Zynamics公司
创始人

MikkoHypponen
CRO of F-Secure



SaumilShah
Founder and CEO
of Net-Square

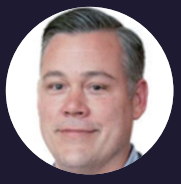
埃胡德·巴拉克
以色列前总理
前国防部长

阿纳托里·斯米尔诺夫
俄罗斯国际信息安全协会
理事长

INTERNET SECURITY CONFERENCE

奥列格·赫拉莫夫
俄罗斯联邦安全会议
副秘书上将

爱德华·吉约
法军总参谋部
海军上将



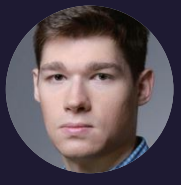
Brian Gorenc
ZDI计划
负责人

Holger Unterbrink
思科Talos
技术主管

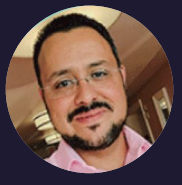
Erez Kreiner
前以色列国家信息
安全局局长
前以色列国家
网络安全委员会主任

Denis Davydor
俄罗斯安全互联网联盟
主席

Neil Walsh
联合国毒品与犯罪问题
办公室 (UNODC)
网络犯罪全 球项目主管

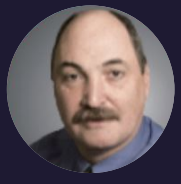


Boris Larin
卡巴斯基实验室
启发检测和漏洞
研究小组资深恶意软件
分析师



Barny Sanchez
IBM安全事业部
威胁防护与认知安全
首席技术官

Jay Heiser
Gartner
研究副总裁、
安 全分析师



James A. Lewis
美国智库战略
与国际研究中心
(CSIS)高级研究员、
技术和公共政策项目主任

Costin-Raiu
卡巴斯基全球研究
分析团队GReAT
负责人

Derek Manky
Fortinet
全球安全战略官

Rave Cohen
以色列国家反恐局
(CTU) 安全信息
总负责人

Gottesgnade Ophir
以色列8200部队
前开源分析部门主管

企业、技术专家

他们曾在ISC探讨安全技术，分享成功经验

企业CXO

周鸿祎
ISC大会主席
360集团董事长
兼CEO

叶健
360集团首席运营官
360政企安全集团
首席执行官

胡伟武
龙芯中科技术有限公司
董事长

于海波
天融信科技集团
董事长

范渊
杭州安恒信息技术
有限公司董事长
兼CEO

卜峥
滴滴信息安全
副总裁

余虎
华为云
首席战略官

文坊
启明星辰集团
高级副总裁 合伙人

罗东平
山石网科董事长
兼CEO

白小勇
北京炼石网络技术
有限公司创始人 CEO

马坤
西安四叶草
董事长

张瑞冬
成都无糖信息技术
有限公司
创始人 CEO

蔡晶晶
永信至诚董事长
i春秋校长

董靖
思睿嘉得 创始人

方兴
全知科技创始人

INTERNET
SECURITY
CONFERENCE

行业专家

谭晓生
北京赛博英杰
科技有限公司
创始人、董事长

李雨航
云安全联盟
大中华区主席
联合国WSF数字经济
研究院副院长

翟起滨
中国科学院数据与通信保护
研究教育中心
教授/博导

杜跃进
360集团
首席安全官

王文海
浙江大学求是特聘教授
国家万人计划科技创业
领军人才 国家重点研发
项目首席科学家

夏鲁宁
数字认证首席科学家
研究院院长

潘剑锋
360首席科学家
国家信息安全漏洞库
特聘专家

秦安
中国网络空间战略
研究所所长

潘柱廷
北向智库首席经略师

吴铁军
绿盟科技伏影实验室
负责人

范霁红
国家电投集团科技
创新总监
中央研究院党委书记
董事长

刘建伟
北京航空航天大学
网络空间安全学院
院长

王铁磊
盘古团队
联合创始人

程光
东南大学网络空间
安全学院 院长

于挺
卡塔尔计算研究所
网络空间安全组
负责人

数 字 安 全 的 领 导 者

360政企安全

数 字 安 全 的 领 导 者

360政企官网

360政企公众号

www.360.net

客服热线：400-0309-360

售后邮箱：service-tech@360.cn

360政企安全集团内刊