

ZERO TRUST SUMMIT

QINGDAO, CHINA JUNE 25, 2021 中国·青岛

第二届国际零倍任峰会

数字时代:零信任剑行天下

云原生与SASE 零信任新框架新思考

单位: CSA大中华区多云安全工作组组长 360未来安全研究院 云安全研究院副院长

主讲人:魏小强



01 数字时代面临的安全挑战

02 未来安全需要一个新的框架

03 基于零信任的SASE框架实践与思考

云优先、移动优先时代来临

The cloud will be our new data center and the internet our new network.

一切皆可编程

每年新增代码1110亿行* , 零代漏洞1个/天**

漏洞不可避免,漏洞无处不在

- *《应用程序安全性报告》Secure Decisions。
- ** 2015年1个/周, 2021年1个/天





万物均要互联

2025年预计将有416亿个IoT设备*

网络威胁目标指数级增长, 单点防护难以为继





软件定义世界

网景公司(Netscape)创始人马克·安德森说:"软件正在吞噬整个世界"

美国工程院院士、C++语言发明人本贾尼·斯特劳斯特卢普说:"人类文明将运行在软件之上"



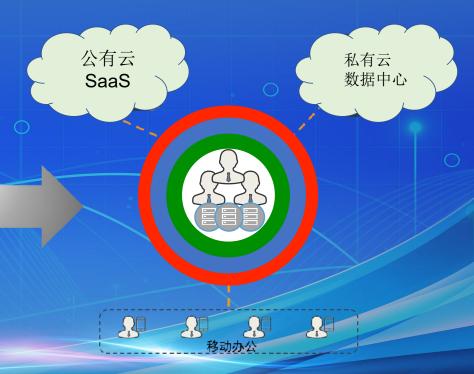


网络边界消失

网络安全边界防护时代

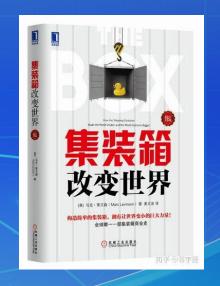


边界消失



云原生时代来临





云原生把云计算的优势发挥到极致

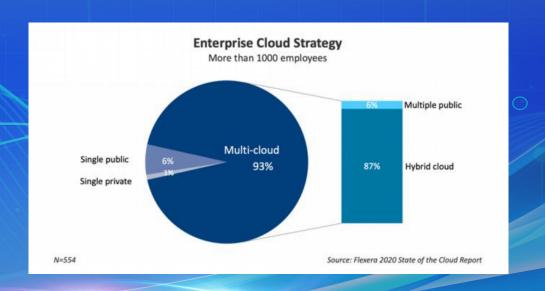
没有集装箱就没有全球化





多云成为数字时代企业的首选战略

- 拥抱云的弹性
- 防止被云供应商锁定
- 保护敏感信息

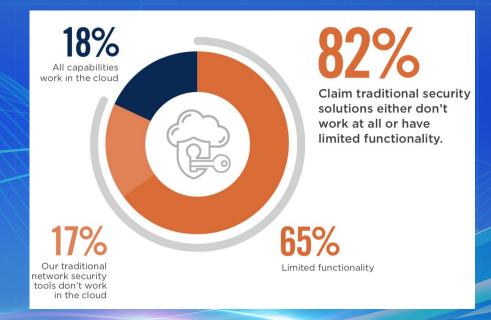






多云时代,传统安全日渐式微

适配困难 网络延迟 安全盲点 缺乏弹性 管理复杂



Source: 2020 Cloud Security Report





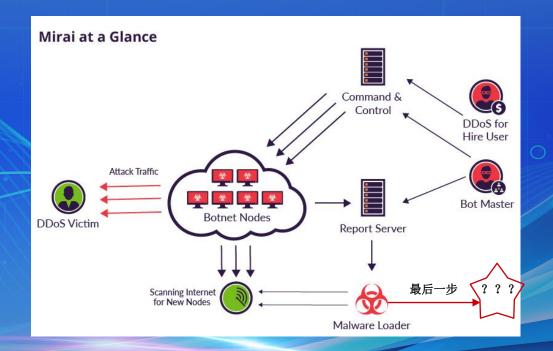
未来安全

安全和每个人相关



Mirai僵尸网络攻击

Mirai是一种恶意软件,它将运行Linux的联网设备变成远程控制的机器人。然后,这些设备被用作大规模网络攻击的僵尸网络的一部分。它主要打击在线消费设备,如IP摄像机和家用路由器。2016年,威胁者利用Mirai和Bashlight发起了多次直接拒绝服务(DDoS)攻击,导致主要服务瘫痪。也会导致了收入损失和品牌声誉受损。



行业分类和开源

INDUSTRY SECTORS AND OPEN SOURCE

Percentage of Open Source in Codebases, by Industry



Aerospace, Aviation, Auto. Transportation, Logistics



Big Data, Al, Bl. Machine Learning



Computer Hardware and Semiconductors



Cyber Security





Energy and Clean Tech



Enterprise Software/SaaS



Financial Services and FinTech



Healthcare, Health Tech, Life Sciences



Internet and Mobile Apps



Internet and Software Infrastructure



Internet of Things



Manufacturing, Industrials, Robotics



Marketing Tech



Retail and E-Commerce



Telecommunications and Wireless

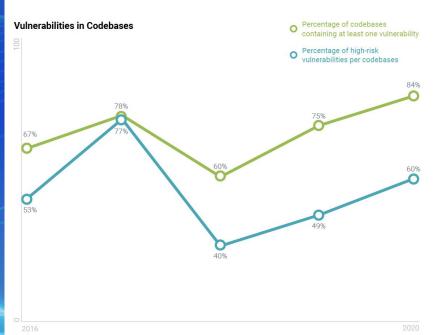


Average of 91 Codebases Audited per Industry





开源代码库中的漏洞情况



至少包含一个漏洞的代码库占比

每个代码库中高风险漏洞占比



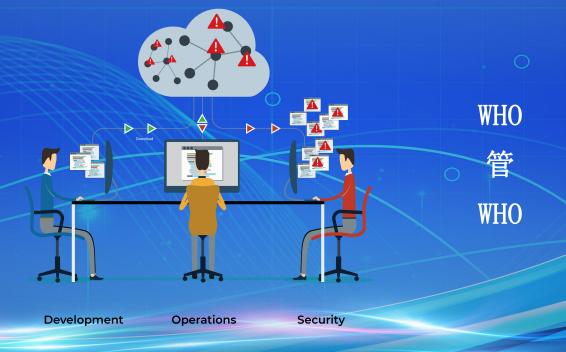


01 数字时代面临的安全挑战

02 未来安全需要一个新的框架

03 360 基于零信任的SASE框架实践

应对未来安全挑战需要一个新网络安全框架

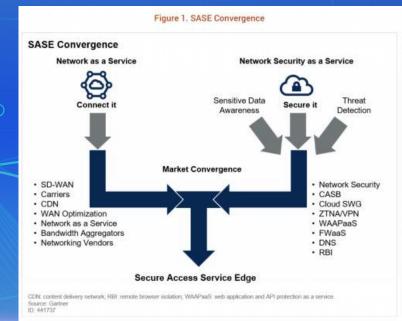






如何理解SASE

Gartner SASE架构融合了网络和安全服务到一个统一的云平台上,包括SD-WAN,安全Web网关,CASB,SDP,DNS保护和云防火墙服务,以用户的身份,应用,设备和应用为中心。



融合。身份驱动

云原生

全球化

任何边缘

2021 第二届国际零倍任峰会



构建SASE框架的思路

- 关于网络攻击的"硬道理":没有人能免于网络攻击。必须加强在事件发生时的应对能力
- 转向零信任: 基于风险评估的方法, 识别高价值资产帮助企业迈出零信任的第一步;
- 构建全域防御策略:通过SASE安全框架保护IT和OT网络,物理世界与虚拟世界已经打通
- 保持战略性和长期性:实现零信任任重道远,提高网络安全现状的基线。



SASE的本质是把安全从信息化中解藕





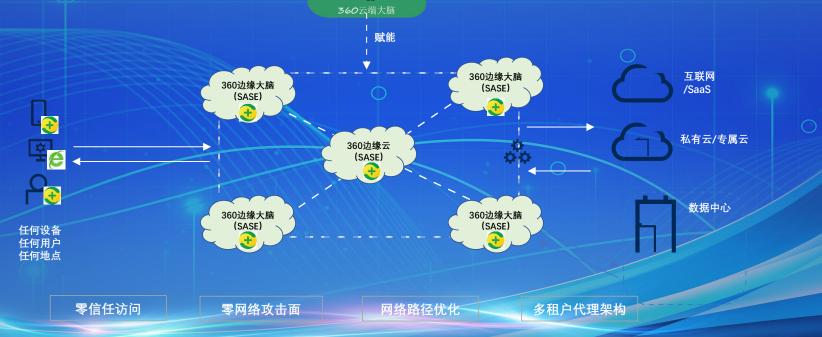


01 数字时代面临的安全挑战

02 云原生安全需要一个新的框架

03 360 基于零信任的SASE框架实践

360基于安全大脑赋能的零信任框架:让安全零用水用电一样方便







360 零信任安全实践

威胁情报能力

安全大脑

安全浏览器

安全运营能力

安全算力(150)

安全大数据平台

密码认证体系

实战攻防能力

安全专家



东半球最强的白帽子军团

200人的安全精英团队,超3800人的安全专家团队

对手从病毒作者到犯罪组织、APT、网军,磨炼形成东半球最强大的白帽子军团

3连续四年封神问鼎MSRC安全精英榜



14个技术研究团队



360 Vulcan Team



360 Sky-Go Team



360 Alpha Lab



360 Gear Team



360 MeshFire Team



360高级威胁应对团队



360NetLab



360 Vulpecker Team



360 Okee Team



360 Nirvan Team



360 QVM Team



360烽火实验室



360冰刃实验室



360白泽实验室





10个研究机构

360 漏洞研究院

360 高级威胁研究院

360 工业互联网安全研究院 360 网络安全研究院

360 AI安全研究院

360 云安全研究院 360 安全工程研究院

360 数据安全研究院

360 天枢智库

360 标准化部

5. SURESH CHELLADURAL 8. YANGKANG OO 9. CAMERON VINCENT 10. XUEFENG LI™ 13. KE LIU (@KLOTXL404)P 14. FANGMING GU 600 15. WTM # 16. JIADONG LU∞ 17 MARKUS WULFTANGE 19. PHAM VAN KHANH 20. JEONGOH KYEA 21. IVAN VAGUNIN*® 22. ABDUL-AZIZ HARIRI 22. JAANUS KÄÄP 24. GUOPENGEEL 25. HAIFEI LI 29. CVIEW 30 GILDABAH

3. YUKI CHEN ***

4. ASHAR JAVED

26. MARCIN 'ICEWALL' NOGA

27. 男人至死是少年

30. SOROUSH DALILI (@IRSDL) 32. WILLI 33. ZHANGJIE

34. ANDREA PIERINI 34. SIMON BARSKY 36. SORRYMYBAD

38. CHRIS DANIELI 39. OUAN IIN

40. ANDREA MICALIZZI AKA RGOD 40. MEYSAM FIROUZI 40. NETANEL BEN-SIMON

40. YOAV ALON 44. DHANESH KIZHAKKINAN 44. KOSHL 46. ANONYMOUS

High Impact

46. SHIH-FONG PENG * 8

2. ZHINIANG PENG (@EDWARDZPENG) 46. WAYNE LOW 46. ZHIYI ZHANG 50. MOON LIANG

MSRC Most Valuable Security Researcher

2020

52. OMER TSARFATI 53. WENGUANG JIAO

54. OSKARS VEGERIS 54. SHLII 54. ZHANG SEN 8 *

57. ZHIPENG HUO 58. VIKAS ANIL SHARMA

59. HONGZHENHAO 61. STEVEN SEELEY (MR_ME)

DI WENGUNWANG 63 HURENIN S

64. ABDULRAHMAN ALQABANDI

66. YING XINLEI® 67. SEFA ALTIN

68. HÀ ANH HOÀNG 68. LE HUU QUANG LINH

70. DIRK-JAN MOLLEMA 71. MARCEL BILAL

72. CLÉMENT LAVOILLOTTE 73. WENXU WUS 74. ANAS LAABAB

74. JOSIP FRANJKOVIĆ ®

78. MOHAMED HAMED @ . 78. YHZX 2013 78. ZHANG WANGJUNJIE

78. ZHUNKI 85. CLÉMENT LABRO 86. ANONYMOUS

87. BAR LAHAV 88. HUÝNH THÔNG

90. ANONYMOUS 91. DANG THE TUYEN

Researchers working with Trend Micro's Zero Day Initiative





360以安全大脑为核心算力中心的安全能力

最大中文漏洞库 总漏洞超过**40**万 每天新增可达**500**个



立体式主防库

覆盖**5**亿客户端 总日志数**50000**亿

每天新增**100**亿

最大的存活网址库 覆盖国内96%客户端50000亿条 每天查询300亿条





互联网域名信息库 90亿DNS解析记录 每天2000亿次DNS解析 每天新增100万个



海量页面访问数据库 17 亿个页面访问数据

服务10亿用户,终端安全软件全覆盖,积累全球独有不可复现的大范围、长时间、多维度安全大数据

25万台服务器 6万台计算服务器 109个数据中心 总存储数量超2EB 每天新增超过1.5PB 数据维护费用每年超5亿

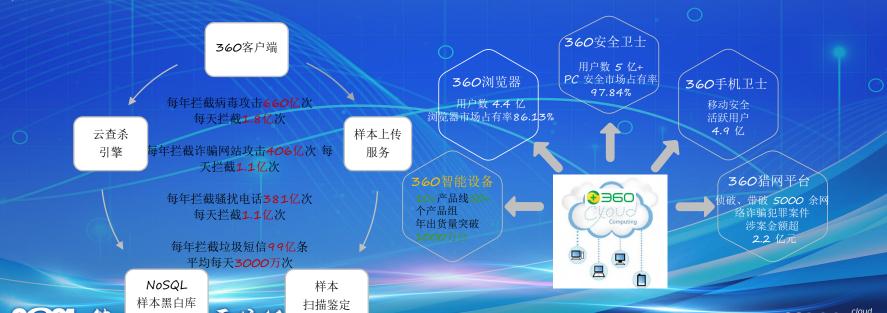




全球率先采用云端大数据分析技术实现安全查杀

当时,云端查杀这一颠覆式技术创新,超越了传统杀毒软件的技术思路,为商业模式创新奠定基础。

今天,基于云的服务模式已成全球趋势,知识与情报驱动的安全离不开云端大数据分析,云端订阅模式成主流



GREATER CHINA REGION alliance

360 XaaS 服务:原生安全 一切即服务









QINGDAO, CHINA JUNE 25, 2021 中国·青岛

第二届国际零倍任峰会

数字时代:零信任剑行天下

《多云安全风险图谱解读》解读

多云安全风险图谱白皮书的编制背景

1、企业比以往任何时候更多开启多云战略来增强其数字化转型中的竞争力和应对突发算力不足对其业务流程的影响。对多云应用场景和多云安全风险的深入研讨,对组织、政府、城市等实现数字化转型、增强竞争力,优化生产力,保护数据安全等具有非常重要的意义。

2、CSA-GCR于2021年3月31日成立多云安全工作组,凝结行业众多领先企业的优势力量,基于实战经验和研究积累,致力于助推多云安全技术在产业加速落地应用,为组织面临的多云场景下的安全挑战提供应对策略。多云安全工作组的工作目标是致力于提供产业合作平台,凝聚行业共识,解决企业上云所面临的安全问题,促进云安全生态的健康发展,助力中国企业成功实现数字化转型。



《多云安全风险图谱》: 多云的典型应用场景

本地负载的弹性扩展

多云数据备份

多云主备容灾

构建跨国跨区域系统

多云数据分类存储

多云开发测试生产分离

多云异构融合

多云改善用户体验





《多云安全风险图谱》:多云时代面临的八大安全风险***



多云安全人才不足

多云安全集成风险

多云环境攻击面扩大

多云安全可见性缺乏

多云迁移安全风险

多云安全治理风险

多云安全合规风险

多云安全配置风险

*CSA 《多云安全风险图谱》2021.6





多云安全风险图谱发布给行业带来的意义

- 1、国内首次联合多家业内企业共同书写的多云安全风险图谱白皮书,帮助各个组织在制定和启动多云安全战略时提供有价值的指导和参考。也是行业首家专门针对多云安全风险的研究成果。
- 2、该白皮书帮助企业在制定多云安全战略时考虑应用场景和制定安全风险防御策略提供参考。
- 3、首次联合国内多家企业的专家协同通过,经验共享,共同推动产业进步的一次成功尝试。本研究为启动解决复杂的多云安全问题研究课题完成了第一步非常重要的基础工作。





感谢编制组专家的用心付出

本白皮书由CSA大中华区多云安全工作组专家撰写,感谢以 下专家的贡献:

组长: 魏小强

贡献者名单: 于继万 李程 彭汝张 杨天识 朱青 谢江

贡献单位: 360、华为、深信服、e签宝、启明星辰、新华三

观安信息

研究助理:赵晨曦(以上排名不分先后)



多云安全风险图谱

Multi-Cloud Security Risk Map





下载, 2024维码









QINGDAO, CHINA JUNE 25, 2021 中国·青岛

第二届国际零倍任峰会

数字时代:零信任剑行天下

《云安全现状、挑战和安全事件》报告解读

《云安全现状、挑战和安全事件》中文版翻译背景

- 1、企业上云已经成为实现数字化转型的必选项。本报告企业比以往任何时候更多开启多云战略来增强其数字化转型中的竞争力和应对突发算力不足对其业务流程的影响。对多云应用场景和多云安全风险的深入研讨,对组织、政府、城市等实现数字化转型、增强竞争力,优化生产力,保护数据安全等具有非常重要的意义。
- 2、CSA-GCR于2021年3月31日成立多云安全工作组,凝结行业众多领先企业的优势力量,基于实战经验和研究积累,致力于助推多云安全技术在产业加速落地应用,为组织面临的多云场景下的安全挑战提供应对策略。多云安全工作组的工作目标是致力于提供产业合作平台,凝聚行业共识,解决企业上云所面临的安全问题,促进云安全生态的健康发展,助力中国企业成功实现数字化转型。



《云安全现状、挑战和安全事件》报告三大关键发现 😷



- 1. 一个越来越复杂的云场景会持续出现 (63%的调查对象表示在公有云上会运行他们至少41%的工作负载)
- 2. 对许多企业来说,云供应商所提供的安全控制手段是不够的。 (71%的调查对象表示)
- 3. 企业正在寻找补充其人力的自动化安全工具。 (如资产测绘,主动风险监测,跨域自动化管理等)



感谢编制组专家的用心付出

本白皮书由CSA大中华区多云安全工作组专家撰写,感谢以下专家的贡献:

组长: 魏小强

贡献者名单:于继万、秦益飞、吴潇、李吉祥

贡献单位: 360 华为 易安联 天融信 海尔

研究助理: 赵晨曦(以上排名不分先后)

云安全现状、挑战和安全事件





CSACCR cloud security
GREATER CHINA REGION alliance *



QINGDAO, CHINA JUNE 25, 2021 中国·青岛

第二届国际零倍任峰会

数字时代:零信任剑行天下

Thank You

