Tencent 腾讯 | 腾讯云 | 腾讯安全云鼎实验室 TENCENT SECURITY YUNDING LAB

大型集团云上安全建设实践分享

腾讯安全副总裁、腾讯云鼎实验室负责人

董志强

一次安全演练的复盘总结

防护系统	开发安全	办公网安全	应急响应	外报漏洞	客户协防
日均拦截攻击3669w次，峰值5597w次； 封禁ip共23051个，日均封禁443个。	日均前置检测3017个安全风险； 抢在攻击者之前收敛风险。	日均拦截154封钓鱼邮件； 响应处理8起木马感染。	日均响应190起入侵告警，分析入侵事件24起，紧急止损1起，及时控制风险。	演练期间从外部收集漏洞52个，高危15个。	协助客户15家，开展了33次重要应急， 协助客户处置外部情报135例，封禁攻击ip7447个。

通过实战，总结的风险和攻击趋势

云环境

“两高一弱”依旧是最大高危攻击入口

失效或错误配置导致的攻击快速上升

AK/SK和重要凭据的泄露是重要风险

应用代码安全漏洞对抗是长期工程

办公网络

影子资产（非安全管控资产）风险巨大

钓鱼邮件依旧是办公环境主要攻击方向

违规外联/接入带来巨大潜在风险

供应链

下游供应链：交付软件包/源代码包含AK/SK导致泄露，代码缺陷被研究

上游供应链：开源组件漏洞治理是长期工程

人员及服务外包：人员可信管理、工作环境管控、服务交付物管理需尽早评估规划

腾讯云安全治理架构和组织体系

腾讯云安全合规建设

到今天，腾讯云在全球范围内获得了400+合规资质的认可，覆盖了中国、东南亚、东北亚、欧洲等主流区域，为腾讯云客户业务的全球发展提供了强有力的支持。同时，也发布了多篇白皮书，使市场及客户可以更加透明的了解腾讯云的合规管控，从而达到合作共赢的目的，与客户一同创造更加合规和安全的云环境。

信息安全管理体系认证	云服务信息安全控制实施指引	公有云个人信息保护认证	个人信息管理体系认证	云安全管理体系金牌认证	系统及组织控制体系鉴证
支付卡行业数据安全标准认证	网络安全等级保护-四级	用户数据保护能力-增强级	网信办云计算服务安全评估	ITSS认证	能力成熟度模型集成
新加坡多层云安全标准-Level 3	新加坡数据保护信任标记认证	新加坡银行协会OSPAR审计	韩国信息安全保护管理体系	欧洲数据保护行为准则自评估	德国云计算合规性控制目录

腾讯云平台防护总体架构：高安全等级架构

网络边界安全

天幕批量漏洞防御

防DDOS

云防火墙

应用负载与数据安全

VPC

身份与特权管控

CAM访问管理

细粒度权限 | SSO | 联合身份 | 多因素认证

BH堡垒机

特权管控 | 高危拦断 | 操作审计 | 审批授权

HSM 国密加密

SSM凭据托管

CAM集成 | 凭据加密 | 凭据轮换 | 白盒加密

账号风控

账号安全 | 行为管控 | 情报联动

Subnet

应用负载运行安全

应用交付与访问安全

黑白网关 | WAF | CLB | EdgeOne

应用运行环境安全

CSPM 云安全态势管理

CIEM 身份与配置安全 | CWPP 云工作负载保护 | CSNS 容器网络安全

镜像安全 | 容器虚拟化隔离

数据安全

应用数据安全

细粒度访问控制 | 细粒度国密加密 | 数据脱敏 | 数据访问审计

安全传输

国密SSL | 双向证书 | SSL卸载 | 默认加密

数据安全治理

数据分类分级 | 数据风险评估 | 数据安全态势

安全存储

KMS | Cloud HSM | 存储默认加密

安全计算

TEE安全计算 | 国密SDK | 抗量子加密

安全管理与运营

主动风险检测

高危端口服务 | 外部暴露面 | 应用漏洞扫描 | BAS持续验证 | 错误云配置 | 40+项

持续风险监控

账号异常 | 访问异常 | 日志审计 | 外部威胁情报 | 攻击告警 | 网络异常 | 组件和代码安全 | 软件供应链安全 | 60+类

智能安全分析

云平台SOC | 安全数据湖 | 安全大模型策略引擎

自动化运营工作流

情报研判 | 一键封堵 | 漏洞扫描 | 应急响应 | 数据分类分级 | 100+工作流

安全指标看板

安全运营大盘 | 平台风控指标 | 平台安全指标 | 应用安全指标 | 数据安全指标

应用开发安全

Coding DevSecOps 集成平台

需求设计	代码编写	代码准入	集成打包	自动化测试	预发布	发布	运营
敏捷威胁建模 • 建模工具库 • 安全设计基线 • 半自动化评估 • 安全设计评审 • 安全培训和考试	代码安全检查 • 安全编码规范 • SAST • SCA • 敏感信息检测	代码安全检查 • SAST • SCA • 敏感信息检测 • 人工代码审计	制品安全检查 • 容器镜像扫描 • APK包扫描 • 织云包检查	应用安全扫描 • DAST测试 • IAST测试 • MAST测试 • 安全漏洞扫描	环境安全检查 • 安全配置基线 • 安全基线评估 • 系统组件评估 • 安全漏洞扫描 • 渗透测试	服务风险检查 • 高危服务监控 • 通用漏洞检查 • 应用组件风险 • WAF安全策略 • 证书及加密管理	安全监控和应急 • 入侵监测 • 安全巡检 • 情报监控 • 漏洞管理 • 红蓝对抗

基础设施安全

高可靠基础设施

可信计算	机密计算	虚拟化与安全操作系统	高性能云网络	高可用基础设施
• 安全加固的自研星星海服务器硬件 • 可信启动，加固的安全系统层 • 持续度量，端到端的可信基础设施	• 硬件隔离的机密计算 • 抽象TEE架构，支持多种硬件 • 信创支持的机密计算	• 硬件隔离虚拟化 • 安全加固的虚拟化层 • EAL4+安全操作系统	• 100Gbps+实时传输 • 千万级高并发 • 500G+流量清洗	• 50+可用区 • T3+数据中心，三副本存储 • 单实例服务可用性99.97 5%，数据可靠性99.99 999 99%

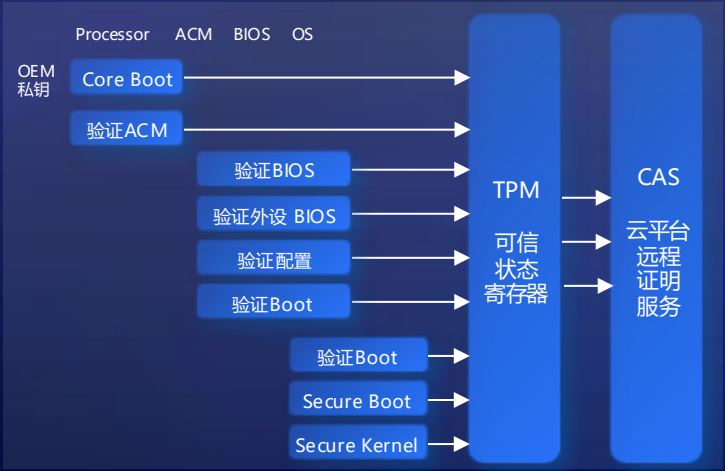
高安全等级架构：全栈可信基础设施

高安全等级架构：可信计算架构与硬件供应链安全保证

通过服务器硬件安全优化、可信计算技术与供应链安全保证云基础设施安全。

可信硬件体系

通过CPU及独立安全芯片TPM2内置双可信根（Root of Trust for Measurement），确保系统硬件环境完整性和可信计算环境，通过BootGuard等技术确保系统可信启动，内核完整性保护和TXT技术保障软件计算环境安全，结合可信云网络实现端到端可信隔离。



硬件/固件安全设计、加固与审计

通过自主服务器设计ODM和供应链安全保证服务器和云基础设施安全性，对硬件设计、芯片功能和固件功能进行裁剪和安全审计防止硬固件开发过程导入的漏洞风险，实现最小化安全TCB（Trusted Computing Base）。

- 服务器组件优化裁剪
- Boot Guard
- Secure Boot
- BIOS签名与校验
- 固件刷新保护
- IPMI防火墙
- 高性能智能网卡
- TXT/TPM2
- 硬件/固件安全设计分析
- 固件安全审计和渗透测试

高安全等级架构：内核0day防御+应用热补丁

对云底座操作系统和虚拟化平台进行安全加固，确保底层安全可靠。

内核0day防御

- 研发0day检测防御能力，内部关键业务机器部署，有效防范未知风险
- 历史漏洞复测，防御率93%；实战对抗演练中发挥重要作用

可防	泄漏方式	缓解绕过&控制流劫持	权限提升	exp
1	/	UAF、堆喷struct pid、竞争条件	注入setuid程序	2021: "How a simple Linux kernel memory corruption bug can lead to complete system compromise" by Jann Horn [article] [CVE-TBD]
0	/	/	/	2021: "SuDump: Exploiting suid binaries through the kernel" by Itai Greenhut [article] [CVE-TBD]
1	eBPF map任意读	堆喷eBPF map覆盖op指针	commit_creds	2021: "CVE-2021-34866 Writeup" by HexRabbit [article] [CVE-2021-34866]
1	eBPF map堆喷	eBPF指令	覆盖cred内存	2021: "Kernel Pwning with eBPF: a Love Story" by Valentina Palmiotti [article, CVE-2021-3490]
1	/	ret2usr	ret2usr, commit_creds	2021: "CVE-2017-11176" by Maher Azzouzi [article] [CVE-2017-11176]
1	eBPF map堆喷	UMH劫持	UMH劫持	2021: "Sequoia: A deep root in Linux's filesystem layer (CVE-2021-33909)" by Qualys Research Team [article, CVE-2021-33909]
1	sk_buff堆喷	pipe_buf堆喷	ret2usr, commit_creds	2021: "CVE-2021-22555: Turning \x00\x00 into 10000$" by Andy Nguyen [CVE-2021-22555, article]
0.5	ctl_table堆喷	内核态部署可执行shellcode	commit_creds	2021: "Exploitation of a double free vulnerability in Ubuntu shiftfs driver (CVE-2021-3492)" by Vincent Dehors [article, CVE-2021-3492]
1	eBPF map堆喷	UAF堆喷	文件描述符劫持	2021: "CVE-2021-20226 a reference counting bug which leads to local privilege escalation in io_uring" [article] [CVE-2021-20226]
1	dmesg	竞争条件、isotp_sock堆喷	UMH劫持	2021: "CVE-2021-32606: CAN ISOTP local privilege escalation" [article] [CVE-2021-32606]
1	/	user ns、sendmsg堆喷	UMH劫持	2021: "CVE-2021-3609: CAN BCM local privilege escalation" [article] [announcement] [CVE-2021-3609]
1	/	user ns、漏洞接口调用	namespace劫持	2021: "SSD Advisory – OverlayFS PE" [article] [CVE-2021-3493]
1	eBPF map堆喷	竞争条件、UAF	覆盖cred内存	2021: "CVE-2021-20226: A Reference-Counting Bug in the Linux Kernel io_uring Subsystem" by Lucas Leong [article] [CVE-2021-20226]
1	特殊函数指针泄漏	iscsi_transport函数指针劫持	UMH劫持	2021: "New Old Bugs in the Linux Kernel" [article] [CVE-2021-27365, CVE-2021-27363, CVE-2021-27364]
1	符号表	竞争条件、UAF、sk_buff堆喷	覆盖cred内存	2021: "Improving the exploit for CVE-2021-26708 in the Linux kernel to bypass LKRG" by Alexander Popov [article] [slides]
1	/	user ns、sendmsg堆喷	覆盖cred内存	2021: "The curious case of CVE-2020-14381" [article] [CVE-2020-14381]
1	伪造waiter泄漏task_struct	pipe_buf堆喷	覆盖cred内存	2021: "Exploiting CVE-2014-3153 (Towelroot)" by Elon Gliksberg [article] [CVE-2014-3153]
1	内核栈地址泄漏	user沙箱、sendmsg堆喷	覆盖cred内存	2021: "CVE-2014-3153" by Maher Azzouzi [article] [CVE-2014-3153]
1	/	竞争条件、UAF	/	2020: "Kernel Exploitation With A File System Fuzzer" [slides] [video] [CVE-2019-19377]
1	/	竞争条件、UAF	/	2020: "CVE-2020-14386: Privilege Escalation Vulnerability in the Linux kernel" by Or Cohen [article] [CVE-2020-14386]
1	eBPF map堆喷	array_map_ops函数指针劫持	覆盖cred内存	2020: "CVE-2020-8835: Linux Kernel Privilege Escalation via Improper eBPF Program Verification" by Manfred Paul [article] [CVE-2020-8835]
1	dmesg	竞争条件、UAF、vb2_buffer堆喷	UMH劫持	2020: "CVE-2019-18683: Exploiting a Linux kernel vulnerability in the V4L2 subsystem" by Alexander Popov [article] [slides] [CVE-2019-18683]
1	tcp socket指针泄漏	UAF、setxattr堆喷	/	2019: "KARMA takes a look at offense and defense: WrongZone from exploitation to repair" [article] [CVE-2018-9568, WrongZone]
1	/	user ns、sendmsg堆喷	ret2usr, commit_creds	2019: "An Exercise in Practical Container Escapology" by Nick Freeman [article] [CVE-2017-1000112]
1	/	user ns、sendmsg堆喷	UAF、堆喷cred	2019: "Analysis of Linux xfrm Module Cross-Border Read-Write Escalation Vulnerability (CVE-2017-7184)" [article] [CVE-2017-7184]
0.5	eBPF map任意读	/	覆盖cred内存	2019: "Analysis of Escalation Vulnerability Caused by Integer Extension of Linux ebpf Module (CVE-2017-16995)" [article] [CVE-2017-16995]
1	/	堆风水覆盖bpf_map_ops	ret2usr, commit_creds	2019: "Linux kernel 4.20 BPF integer overflow vulnerability analysis" [article]
1	/	sendmsg堆喷	ret2usr, commit_creds	2018: "CVE-2017-11176: A step-by-step Linux Kernel exploitation [article] [CVE-2017-11176]
1	dmesg	UAF	UMH劫持	2018: "A cache invalidation bug in Linux memory management" by Jann Horn [article] [CVE-2018-17182]
0	/	/	/	2018: "Integer overflow in Linux's create_elf_tables()" [announcement] [CVE-2018-14634]
0	/	/	/	2018: "MMap Vulnerabilities – Linux Kernel" [article] [CVE-2018-8781]
0.5	eBPF map任意读	/	覆盖cred内存	2018: "Ubuntu kernel eBPF 0day analysis" [article] [CVE-2017-16995]
0.5	eBPF map任意读	/	覆盖cred内存	2018: "eBPF and Analysis of the get-rekt-linux-hardened.c Exploit for CVE-2017-16995" [article] [CVE-2017-16695]
1	/	user ns、sendmsg堆喷	ret2usr, commit_creds	2017: "Linux kernel: CVE-2017-1000112: Exploitable memory corruption due to UFO to non-UFO path switch" by Andrey Konovalov [announcement] [CVE-2017-1000112]
1	半暴力猜解	user ns、堆喷	覆盖cred内存	2017: "Exploiting CVE-2017-5123 with full protections. SMEP, SMAP, and the Chrome Sandbox!" by Chris Salls [article] [CVE-2017-5123]
1	/	竞争条件、UAF	ret2usr, commit_creds	2017: "Race For Root: The Analysis Of The Linux Kernel Race Condition Exploit" by Alexander Popov [slides] [CVE-2017-2636]
0	/	/	/	2017: "Dirty COW and why lying is bad even if you are the Linux kernel" [article] [CVE-2016-5195]
1	堆喷struct file指针泄漏	user ns、file_operations堆喷	ret2usr, commit_creds	2017: "PWN2OWN 2017 Linux kernel privilege escalation analysis" [article] [CVE-2017-7184]
1	dmesg	user ns、任意写	ret2usr, commit_creds	2017: "Exploiting the Linux kernel via packet sockets" by Andrey Konovalov [article] [CVE-2017-7308]
1	dmesg	user ns、任意写	ret2usr, commit_creds	2017: "CVE-2017-6074: DCCP double-free vulnerability (local root)" by Andrey Konovalov [announcement] [CVE-2017-6074]
1	dmesg	user ns、竞争条件、任意写	ret2usr, commit_creds	2016: "CVE-2016-8655 Linux af_packet.c race condition (local root)" by Philip Pettersson [announcement] [CVE-2016-8655]
1	/	user ns、竞争条件、任意写	ret2usr, commit_creds	2016: "Exploiting Recursion in the Linux Kernel" by Jann Horn [article] [CVE-2016-1583]
1	/	UAF、sendmsg堆喷keyring	ret2usr, commit_creds	2016: "ANALYSIS AND EXPLOITATION OF A LINUX KERNEL VULNERABILITY (CVE-2016-0728)" By Perception Point Research Team [article] [CVE-2016-0728]
1	/	UAF、堆喷	ret2usr, commit_creds	2016: "Notes about CVE-2016-7117" by Lizzie Dixon [article] [CVE-2016-7117]
1	/	sendmmsg堆喷skb_shared_info	ret2usr, commit_creds	2016: "CVE-2016-2384: exploiting a double-free in the usb-midi linux kernel driver" by Andrey Konovalov [article] [CVE-2016-2384]
1	/	堆喷subprocess_info劫持函数指针	UMH劫持	2016: "CVE-2016-6187: Exploiting Linux kernel heap off-by-one" by Vitaly Nikolenko [article] [CVE-2016-6187]
0.5	/	UAF、struct file堆喷group_info	?	2016: "CVE-2014-2851 group_info UAF Exploitation" by Vitaly Nikolenko [article] [CVE-2014-2851]
1	针对特定发行版固定偏移量	覆盖proc_root	ret2usr	2015: "Exploiting "BadIRET" vulnerability" by Rafal Wojtczuk [article] [CVE-2014-9322]
0	/	/	/	2015: "Exploiting the DRAM rowhammer bug to gain kernel privileges" by Mark Seaborn and Thomas Dullien [article] [Rowhammer]
1	/	条件竞争、劫持tty_struct.ops	ret2usr, commit_creds	2014: "Exploiting CVE-2014-0196 a walk-through of the Linux pty race condition PoC" by Samuel Gross [article] [CVE-2014-0196]
1	/	user ns	chmod、gid误用	2014: "CVE-2014-4014: Linux Kernel Local Privilege Escalation "exploitation"" by Vitaly Nikolenko [article] [CVE-2014-4014]
1	/	PTRACE寄存器劫持	ret2usr, commit_creds	2014: "CVE-2014-4699: Linux Kernel ptrace/sysret vulnerability analysis" by Vitaly Nikolenko [article] [CVE-2014-4699]
1	kallsyms		覆盖cred内存	2014: "Exploiting the Futex Bug and uncovering Towelroot" [article] [CVE-2014-3153]

- 部署前，漏洞攻击，提权成功：

```
admin-pc@ubuntu:~/tencent$ ./exp
[.] namespace sandbox setup successfully
[.] disabling SMEP & SMAP
[.] scheduling 0xffffffff81064290(0x406e0)
[.] waiting for the timer to execute
[.] done
[.] SMEP & SMAP should be off now
[.] getting root
[.] executing 0x402003
[.] done
[.] should be root now
[.] checking if we got root
[-] something went wrong =(
[!] don't kill the exploit binary, the kernel will crash
```

- 部署后，漏洞攻击，提权失败：

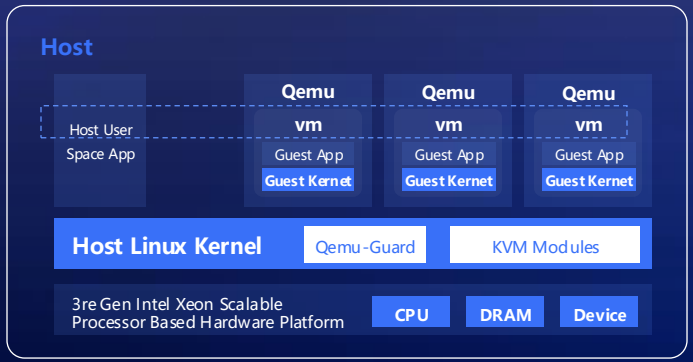
```
admin-pc@ubuntu:~/tencent$ sudo insmod khm.ko
[sudo] password for admin-pc:
admin-pc@ubuntu:~/tencent$ ./exp
[.] namespace sandbox setup successfully
[.] disabling SMEP & SMAP
[.] scheduling 0xffffffff81064290(0x406e0)
setsockopt(PACKET_VERSION): Device or resource busy
```

高安全等级架构：虚拟化逃逸防护

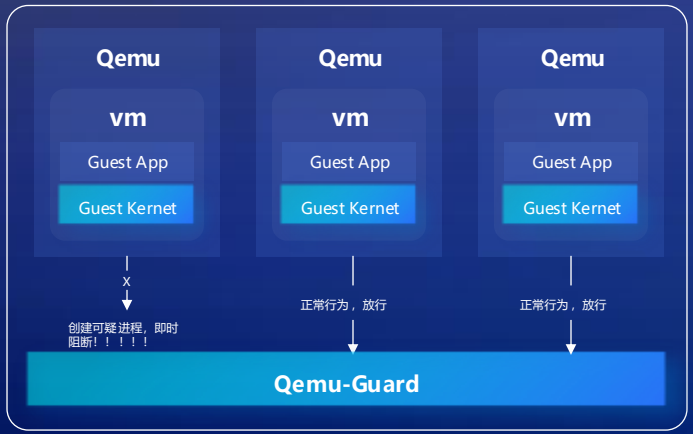
对云底座操作系统和虚拟化平台进行安全加固，通过硬件虚拟化隔离和安全操作系统确保底层安全可靠。

虚拟化逃逸防护

- 针对虚拟化逃逸潜在风险点提前加固，分析环境基线构建白名单，按需部署及灰度运营
- 灵活的观察和拦截能力，具备多种安全模式
- 已在腾讯云全量运行，稳定性、性能和安全性得到充分验证



- Qemu-Guard部署在Host Linux Kernel层，对虚拟化平台各个组件进行监控，阻止非常规行为以及高危敏感操作；及时阻断虚拟化逃逸行为。

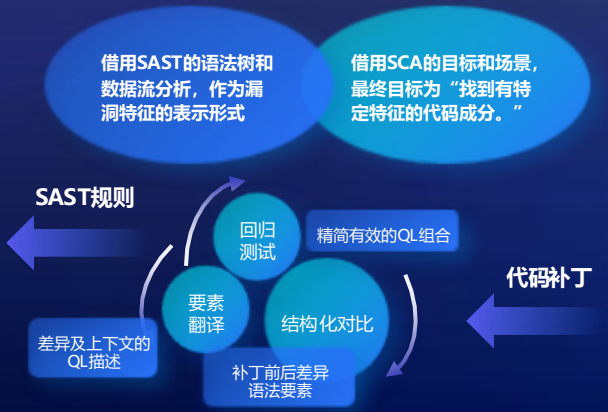


高安全等级架构： 多重机制保障研发安全

安全左移，通过安全组件嵌入、软件成分管理、自动化代码检查和安全有效性测试，层层卡口尽早发现和处置风险，实现“出厂即安全”。

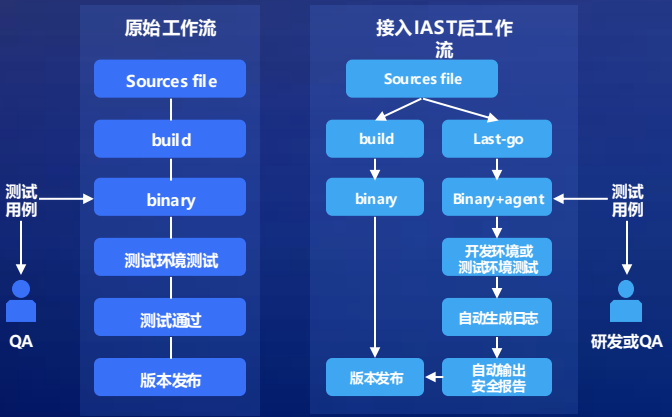
Patch2QL静态代码补丁分析工具

1. 传统静态分析工具基于代码模式匹配，难以回答补丁是否包含的问题
2. 结合SAST和SCA的技术，解决开源生态里补丁分析难题；同时泛化效果有助于发现同类别漏洞
3. 发现微信开源代码供应链安全问题

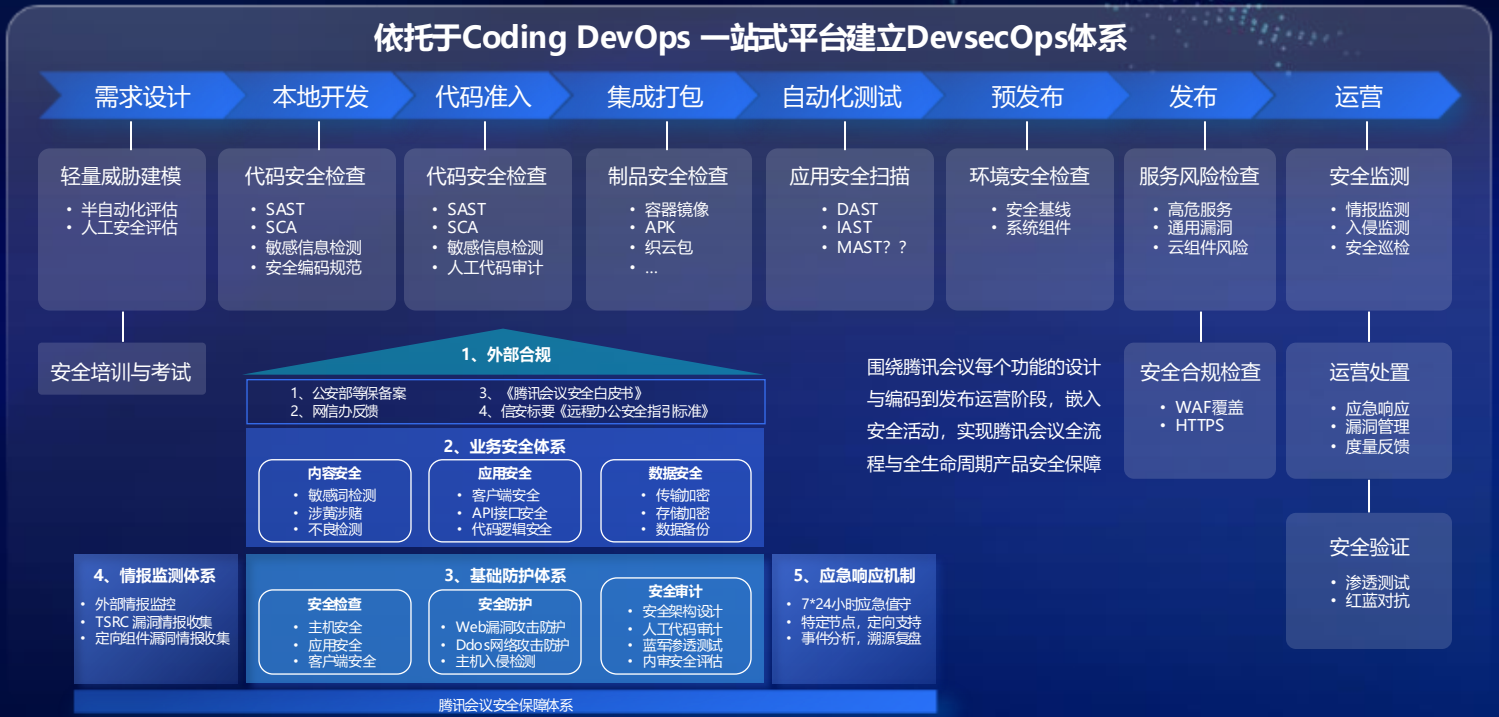


新一代IAST检测工具

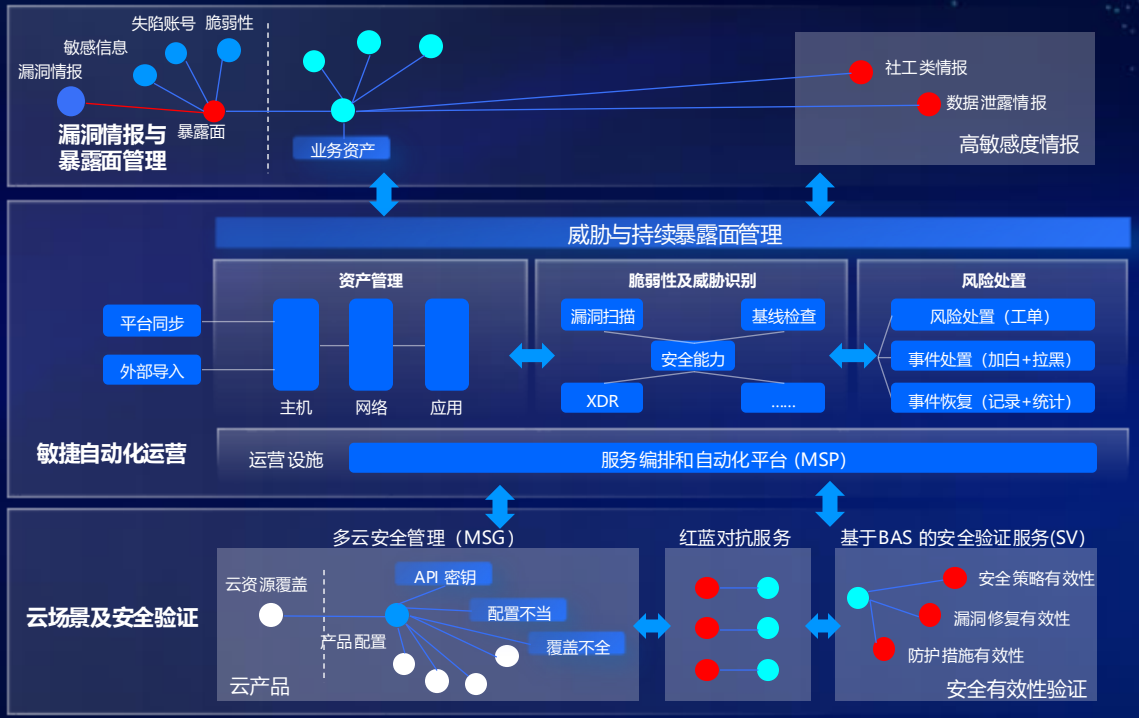
1. 针对云平台主流开发语言golang进行强化，创新性解决协程调用链跟踪问题
2. 代码覆盖率和Race问题检测，成为 golang研发生态最有价值工具
3. 腾讯会议等关键云服务部署应用



案例：腾讯会议DevSecOps实践



高安全等级架构：持续威胁暴露面管理能力



能力1：漏洞情报服务[VI]

能力定位： 最新风险极速感知与发现
能力SLA： 7*24小时，MTTD<30min
应用场景：
1、提前感知业务最新漏洞威胁
2、提供PoC复现以及资产关联分析

能力2：暴露面管理服务(EM)

能力定位： 持续威胁与暴露面管理
能力SLA： 7*24小时，MTTD<8h
应用场景：
1、应用SOAP平台实现暴露面挖掘过程编排，提升覆盖度及时效
2、攻击者视角，覆盖5类攻击面元素

能力3：多云安全管理[MSG]

能力定位： 云安全基线风险的持续控制
能力SLA： 多云暴露面，MTTD<15min
应用场景：
1、云产品安全配置不当导致数据泄露
2、为基线可变性风险提供详细建议

能力4：安全验证服务[BAS]

能力定位： 安全控制措施的有效性验证
建设目标： 按需，MTTD<20min
应用场景：
1、安全演习、历史常见高危漏洞验证
2、WAF绕过、EDR检测逃逸...
3、社工突破，热点漏洞利用...

高安全等级架构：融合全栈风险智能运营

全局看见、全域风险检测、分钟级处置沉淀云上大数据检测、响应体系

核心目标：
全局看见、全域风险检测、分钟级响应应对高等级威胁

运营闭环

运营闭环、自动化、全覆盖收敛云平台风险

- SOAR流云自动处置
- 运营指标化（分钟级处置）
- SOAR流云自动处置
- 风险大盘（全局查看云平台风险）
- 全局阻断（高危风险）

云风险业务场景

全局覆盖云上风险（全覆盖主机安全、数据安全、应用安全、网络安全、云安全、合规、内鬼等）

- AK/SK泄露
- DLP数据泄露
- 云上勒索
- 云主机入侵
- 内鬼数据泄露
- 云产品反入侵
- AK/SK泄露
- DLP数据泄露
- 用户画像
- 黑客情报
- 国际支付风控
- 云产品配置风险
- 安全管控风险
- 权限处理等

风险检测引擎

风险检测引擎

- 流式引擎
- 机器学习
- 规则可视化
- 流式引擎
- 实时分析
- 自动化编排

数据存储

数据存储（支持大数据、云存储、云数据库、图数据库等结构化和非结构化数据）

- ES分布式存储
- 图数据库
- TDW大数据
- TDSQL云数据库
- 云对象存储
- 其他非结构化存储

统一接入

消息总线接入/数据预处理/数据归一

- Kafka
- 流式消息总线
- Logstach
- 日志实时接入
- 数据预处理
- 数据归一化
- 数据解析
- 数据源归并

原始数据（600+）

资产

- DNS
- IDC
- 域名
- 云上
- IP
- 设备指纹

云基础日志

- 云数据库CDB等
- 控制台访问日志
- 云API
- 云存储日志
- 网络日志
- 云审计日志

安全日志

- 主机安全（云镜）
- 云防火墙
- WAF
- NDR
- ID/PS
- 漏扫

其他生态管控日志

- 安灯管控平台
- 北斗平台
- 云管控平台
- 云运维管控
- Tapd开发平台
- vStation云管控

主机&容器安全：一站式工作负载防护，满足合规、护网等重要场景安全防护。

从**“预防→ 防御→检测→响应”**四个环节，帮助用户构建一站式云工作负载防护体系（主机安全+容器安全）。

从**事前防御、事中查杀、事后溯源**帮助用户在**合规、重保、护网等场景**中提供重要安全能力。

主机安全提供**漏洞防御、文件查杀、事件调查**等核心功能，容器安全提供**镜像安全、集群安全、运行时安全**等核心功能，覆盖容器全生命周期。

用户核心需求

合规需求

满足等保测评，两高一弱：高危漏洞、高危端口、弱口令。

漏洞管理需求

漏洞攻击面管理，支持一键漏洞检测、自动修复等能力

入侵防护需求

重点解决主机入侵实时防护，例如：挖矿木马、暴力破解、漏洞攻击等高频威胁。

资产风险管理

支持混合云统一管理，包括：组件、端口、进程等15类指纹资产风险暴露面管理。

一站式云工作负载防护（主机+容器）

主机安全		容器安全	
资产暴露面	文件查杀	资产管理	集群安全
漏洞管理	入侵防御	镜像安全	运行时安全
安全基线	行为监控	安全基线	容器网络策略
文件完整性	安全策略		

客户端一体化，即开即用

安全能力平台：RASP+ | 多引擎 | 策略框架 | 自动预警 | 情报接入 | 溯源分析

产品核心优势

一键启用，混合云架构

- 主机+容器一体防护，一键启用
- 支持混合云，百万级主机，千万核容器防护实践

多引擎，高性能，高检出

- 腾讯云泰石漏洞引擎、Wedetect网络攻击、TAV反病毒等核心引擎

百亿级样本+全网威胁情报

- 百亿级样本资源+全网威胁情报，云端实时预警

Web应用防火墙：Web应用的“门神”，保护网站、小程序、API等Web应用，防薅防刷防爬

核心优势

解决Web业务（网站、小程序、APP等）的安全稳定问题——接得住大流量，防得住攻击，并通过防薅防刷防爬提升业务健康性；针对金融类业务，可进一步识别API并保护敏感数据

核心优势

- 接入部署能力多样 —— 公有云、混合云、专有云多种接入方式；云原生CLB架构，即开即用、弹性伸缩
- Web基础安全业界领先 —— 智能AI引擎 + 腾讯多年积累自研业务防护引擎，防护精准性高
- 海量实时威胁情报 ——海量威胁情报+ 智能算力识别拦截恶意Bot 流量+API 异常发现
- 小程序独有核心安全能力 —— 私有协议加密，微信同等级弱网加速能力、微信账号安全风控能力

适用场景

等保合规

- Web 基础防护：SQL注入、XSS、CSRF、0-day漏洞防御
- 攻击日志、访问日志留存

攻防演练、重要活动保障

- 云端威胁情报与规则运营，针对0day/1day漏洞的小时级响应；万级IP黑名单、访问控制与地域封禁能力
- 恶意机器人BOT、自动化攻击识别与拦截
- API接口防护与API限流

金融行业数据合规

- API资产发现：自动化识别业务 API 调用关系，全面、持续清点 API 接口，缩小风险暴露面；
- API访问检测：恶意请求、异常访问、账号滥用、敏感数据防泄漏

小程序业务质量优化与防护

- 网络加速：基于微信网关全球加速与就近接入能力，让小程序有机会达到微信同等网络质量
- 数据加密：通过微信自研私有协议二次封装加密，极大提高数据破解和爬取门槛，有效保护企业数据资产。

最佳实践

Step1：梳理Web应用和资产

Step2：把支付、用户、营销、互联网类业务接入到WAF

Step3：开启WAF拦截模式，打开CC防护开关，开启访问日志与攻击日志，清洗攻击流量并留存

Step4：开启BOT管理与API防护，拦截恶意爬虫、刷单与羊毛党，进一步提升业务健康性

Step5：开启小程序安全加速，提升小程序与营销活动的业务质量

东风威胁溯源及主动防御系统：专注于解决新对抗形势下，全方位提升企业风险治理能力

“东风”致力于解决网络攻击闭环，以自动化溯源技术为矛，完整攻击者画像数据为盾，提前斩断攻击杀伤链，破除攻击者匿名性，提升企业安全防御体系自动化闭环能力。

事前

发现

事中

缓解

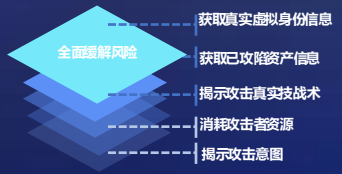
降低

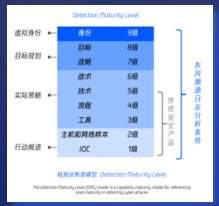
事后

“攻击面管理” 及时收敛风险资产暴露 “东风” 威胁感知模块

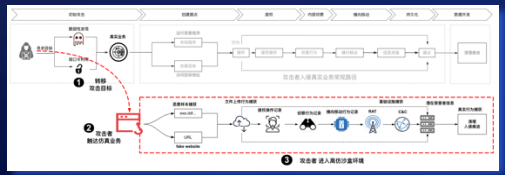
1 脆弱性发现 提前止损

高价值信息 助力**可视化风险行为缓解及预测**





2 干扰攻击路径 及时缓解风险 阻止对真正有价值目标的攻击



- 提升安全运营价值，降低风险；
- 使企业防御体系具备威慑力，缓解风险。

3 从根本上解决攻防对抗最后一公里问题

安全影响

- 商誉损失
- 负面影响
- 无形损失
- 监管罚单

典型威胁案例

- 国有大行遭勒索攻击
- 暗网数据泛滥
- 金融租赁企业遭勒索攻击
- 客户信息泄漏

Xcheck：白盒革命，为DevSecOps而生的新一代SAST白盒产品

DevOps带来全新产品要求，传统白盒难以适配流水线，Xcheck摒弃传统技术路线，腾讯全新自研，实现独家技术突破。

传统白盒产品趋势/痛点

开发模式演进

瀑布/敏捷 → DevOps

白盒使用场景变化

安全独立使用审计平台，返报告 → 流水线集成自动扫描，做门禁

传统白盒痛点

- 速度慢：平均扫描速度在几十分钟，无法适应快速迭代的DevOps开发模式，严重影响流水线效率。
- 误报高：检测报告动辄成百上千个风险，误报过高，强依赖人工审计，无法作为自动化门禁红线。
- 性能差：扫描对内存的占用过大，多任务并发扫描会占用海量资源，无法适应多分支、快迭代的趋势。

Xcheck产品优势

扫描速度快，效率高，对开发友好

- 平均速度每秒5000行
- 不限并发量，98%的任务在1分钟内完成

检出误报低，真正支持流水线门禁落地

23年整体误报率 7.62%

按照严格的误报算法统计

$$\text{误报率} = \frac{\text{忽略} + \text{屏蔽}}{\text{忽略} + \text{屏蔽} + \text{已修复}}$$

Tencent 腾讯 | 腾讯云 | 腾讯安全云鼎实验室 TENCENT SECURITY YUNDING LAB

看得见的安全

SECURITY INSIDE