安全狗
忠诚守护 值得信赖

抗击疫情专题

疫情期间 政府和企业

所面临的网络安全风险如何保障

华南区解决方案专家 蒋竞阳

目录

CONTENTS

01 疫情期间面临的网络安全风险

ONE

工作模式变化带来的安全风险

新型冠状病毒肺炎疫情还在上升阶段，为了防止出现爆炸式扩散，一线二线城市选择只允许机关单位和一类行业返回办公场所开工。但社会仍需运转，经济发展不能停止，诸多条件允许的行业如金融、互联网，选择进行远程网络办公，但远程办公条件下的不可控因素，都可能产生安全风险。

1、因疫情防控需要紧急上线的业务系统或因工作需要临时映射到互联网的业务系统**防护不当**，易遭网络攻击；

2、方便**远程运维**开启服务器3389、22、23等管理端口，易遭勒索软件、蠕虫病毒攻击；

3、开启内部业务网络的**对外访问权限**，易形成安全隐患；

4、缺少VPN、堡垒机等基础安全手段，易产生**接入安全和传输安全**风险；

5、云上办公系统的可能存在**漏洞风险**，容易被利用；

6、远程办公软件**自身的安全**无法保证。

业务互联网化带来的安全风险

随着用户额加快向云端迁移数据、制定新的数字化系统以及增加端点数量，有形资产与数字资产融合进一步融合，**遭受网络攻击**的风险呈指数级增长。

1、业务互联网化为企业经营带来新机遇的同时，也为**网络攻击的扩展和变形**提供了可能；

2、网络攻击方可能通过物联网及云服务扩张**掌握大量的运营数据**；

3、工作场所中**遍布物联网设备**，每个设备都存在潜在安全风险；

4、网络事件的破坏效应会**威胁业务连续性**；

5、**安全漏洞**问题的常因之一是员工；

6、随着交易量不断增加，相关的网络安全**风险数量将快速增长**。

非法的人员蠢蠢欲动

普遍存在的三种攻击情况：以疫情关键字为诱导的**病毒钓鱼攻击**、以疫情为诱饵的信息泄露导致的诈骗攻击、以疫情捐赠为由的携善款跑路的**诈骗攻击**。

一系列电脑版“新型冠状病毒”正在悄然蔓延：

“新冠病毒”一：远程控制 窃取文件

“新冠病毒”二：删除文件 电脑变砖

“新冠病毒”三：黑产不休 变招作祟。

疑似**台湾绿斑黑客团伙**的虚假“疫情统计表格”和“药方”！

那个借新型肺炎对我国发起攻击的黑客组织叫**印度“白象”**！

境外黑客扬言将攻击我国视频监控系统!

南亚APT组织借新冠疫情对我国医疗机构发起定向攻击!

02 疫情期间如何保障网络安全

TWO

如何应对

鉴于目前的现状，很多单位，包括很多单位的部门都选择了远程办公的形式。为了使用单位内网的各类数据和功能，很多时候不得不临时搭建和改造远程办公所用的系统，从而使得**内外网的安全边界被再次打破**，外部安全威胁将**直接威胁内网**的安全。

因此主要围绕在这几个方面来建设：

1、身份权限的准入

2、网络通信的防泄密

3、边界安全的加强

4、管理体系的加强

5、业务系统内部改造加强

……

本质

获取我们有价值的信息、**破坏**我们重要的业务

破坏

获益

目标：所有**承载计算的工作节点**，比如说传统服务器主机系统、虚拟机、私有云计算节点、公有云主机、Docker容器节点以及微服务等，称之为“工作负载”

我们在当前形式下的安全思考?

- 针对黑客的入侵行为，我们能做什么?
- 如何加强资产细粒度管理工作?
- 如何完成纵深防御体系的最后一块拼图，做到基于工作节点全流程事前、事中、事后安全防御体系建设?
- 设备的精准溯源?
- 如何进行系统内部排查，做好脆弱性检查?
- ……

事前　事中　事后

方案一、安全狗·基于工作节点的到工作负载安全解决方案

早发现

通过工作负载安全方案，提前发现对外工作节点存在的**风险薄弱点**，比如说漏洞、弱口令、非法的端口、能做到早发现

早响应

通过工作负载安全方案，当遇到**入侵行为**，甚至于**攻击行为**等，能及时的**早响应**，能有对应的响应处理的能力

早隔离

通过工作负载安全方案，不同的业务之间的出现**非法的访问，异常的行为**，能够及时隔离，能让攻击行为无法藏匿，**早隔离**

早防护

通过工作负载安全方案，提前做好对应的**安全风险的防护**，比如说异常的端口、异常的访问行为，异常的进程，做到**早防护**

方案一、安全狗·基于工作节点的工作负载安全解决方案

主机EDR监测和防护
解决私有云、混合云中主机安全监测及防护问题

云眼

自适应微隔离系统
内部流量精细可视化分析，细粒度安全策略管理

云网

云隙

新一代漏洞补丁管理平台
采用OVAL、NASL标准及相关技术，对主机上面的漏洞、配置缺陷项进行检测发现及修复

云甲

容器安全系统
灵活结合容器编排体系，实现容器全面安全保护

安全狗根据实际的安全场景，结合近几年概念的演进和大量的安全实践，开发出了涵盖主机安全、容器安全、微隔离、补丁管理等安全需求的产品矩阵，形成了安全狗的工作负载安全解决方案

方案特点---动态安全监测及防护

云眼

(云)主机EDR监测和防护
解决私有云、混合云、公有云中各类安全及管理问题

工作负载作为是网络安全中的**最终目标**，也成为了越来越多的用户所面临的最大的安全风险的薄弱点，比如说挖坑木马、勒索病毒、比如说黑客入侵行为，都是在工作负载发生，也是这几年来，众多用户最为头疼的问题。安全狗通过**主机EDR监测和防护**，为用户提供了实时的监测能力，能够快速的发现工作节点层面的安全问题，**动态的进行安全防护**，从而**降低了疫情期间安全风险。**

方案特点---漏洞补丁管理运营

云网

新一代漏洞补丁管理平台
采用OVAL、NASL标准及相关技术，对主机上面的漏洞、配置缺陷项进行检测发现及修复

漏洞补丁管理一直是各个安全和运维人员的关注的问题之一，如何有效**提前发现漏洞，快速的修复漏洞**，也是每个用户最为关注的问题，安全狗通过新一代补丁管理平台，从**windows、linux、中间件、数据库**等多个方面，为用户提供有效的漏洞补丁管理的能力，并能够对接各类重要的运维平台，从而做到漏洞补丁管理运营，在疫情期间做到**风险的提前发现**。

方案特点---自适应精细化安全控制

云隙

自适应微隔离系统
内部流量精细可视化分析，细粒度
安全策略管理

这几年来，越来越多的用户改变自身的传统的架构，比如说it的云化，而架构变化带来最大的风险来自于**东西向流量的风险，**内部威胁，以往很多公司一直依赖防火墙、虚拟本地网和访问控制列表做网络隔离，但是管理方面以及实际效果不够理想。安全狗通过自适应微隔离系统，为用户精细化的识别了流量情况，进行准确的画像，并通过统一的平台，进行了网络隔离安全控制，从而做到了自适应的精细化安全控制。在疫情期间，为用户**区分好各个业务**，做到了**精准的控制**。

方案特点---新环境安全防护

云甲

容器安全系统
灵活结合容器编排体系，实现全面保护

业务互联网化、线上办公的趋势，让容器的技术也被用户慢慢所接受，通过容器的技术，能够有效的提高开发人员和运营人员的效率，但是新技术的采用，也引入新的安全风险。安全狗安全计算环境产品矩阵中的容器安全系统，对容器**全生命周期进行安全管控**，为用户从容器非生产环境和生产环境两个维度考虑，从而做到容器全自动的安全**检测、预警与防护**。在疫情期间，给很多用户**新环境提供有效的防护**手段。

方案二、安全狗·基于工作节点的云磐SECaaS解决方案

多

云磐解决方案提供了**云→服务的完整安全体系**，功能齐全、模块完整，以工作负载为核心，帮助用户可以应对面临的**各种安全场景。**

快

云磐解决方案提供公有云安全服务，**无需额外部署**，无需等待漫长不可控的开发周期，通过在服务器上安装客户端，开通帐号即可使用，**快速响应。**

好

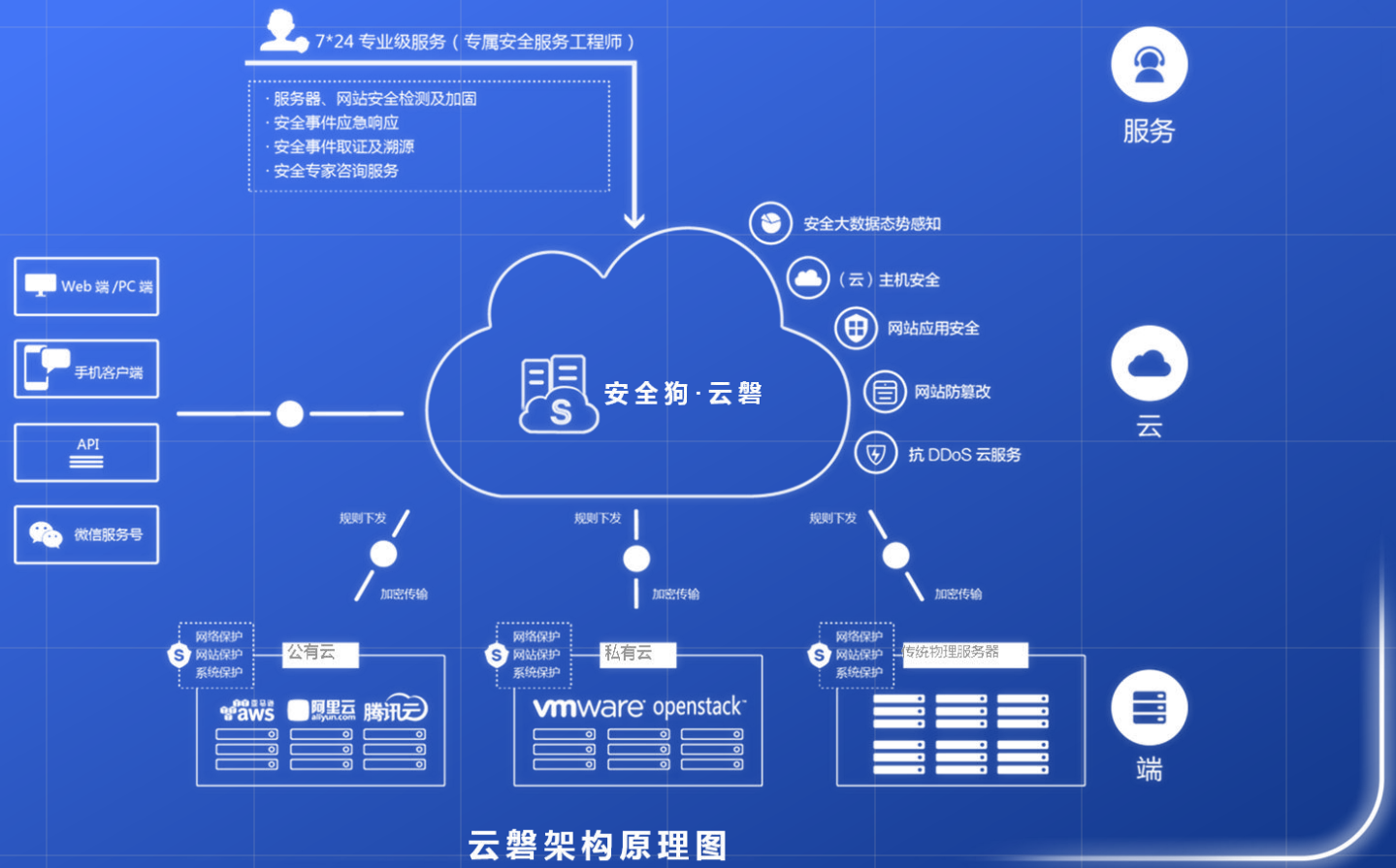
云磐解决方案，从**事前风险评估、事中安全防护及监控、事后应急响应。**通过saas的产品+人工的方式，能很好全面帮助客户解决网络安全风险

省

云磐解决方案既无需占用硬件资源，又可**大大降低投入安全运维的人力**，可以根据实际情况，来选择不同的服务搭配，真正让安全做到**省心省力。**

方案二、安全狗·基于工作节点的云磐SECaaS解决方案

云磐以SECaaS（Security as a Service）安全即服务的模式为用户提供一站式的云安全产品服务平台。包括**（云）主机安全，WEB应用安全，网站防篡改，抗DDoS云服务，安全大数据态势感知等，同时平台配备7*24小时的安全专家服务**，真正为用户构建安全即服务模式的纵深防御产品和服务，为业务发展保驾护航！



云磐架构原理图

7*24专业级安全服务

基于威胁分析驱动和
大数据安全的管理平台
实时监测漏洞风险、攻击威胁

构筑纵深安全防御体系从网络层、应用层到系统层逐级防御和监测实时阻断黑客攻击

云磐SECaaS解决方案

云磐安全服务体系

日志分析及态势感知云服务

云磐融合大数据分析技术、可视化技术、威胁情报技术于一体，为企业构建的新一代云安全管理平台。

- 安全大数据分析，全方位融合安全数据，进行多维度智能分析
- 可视化大屏展示，提供整体态势感知、攻防对抗态势、流量访问态势、威胁事件态势四屏展示
- 态势预测，可发现威胁态势的走向，预见风险，防范于未然
- 威胁情报驱动，依托于安全狗观鸿威胁情报服务平台

(云)主机安全服务

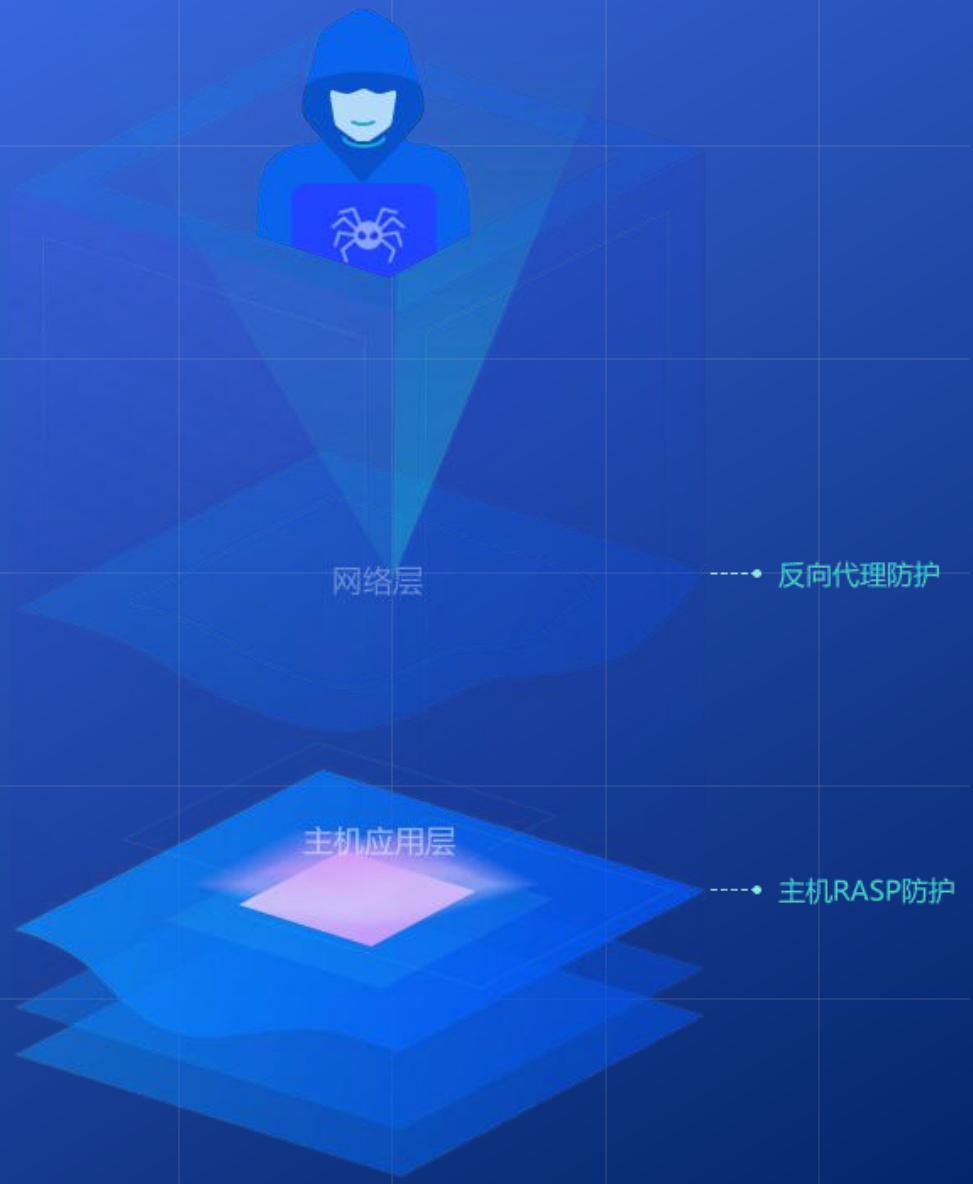
云磐采用先进的端点检测及响应(EDR)技术模型及自适应安全架构相结合的理念思路来构建的新一代（云）主机入侵监测及安全管理云服务系统。

- 解决公有云环境中遇到的安全及管理问题
- 解决新安全形势下数据中心安全问题
- 结合威胁情报进行主机终端异常行为捕获及分析
- 满足（云）等保 2.0 对于主机安全的合规性要求

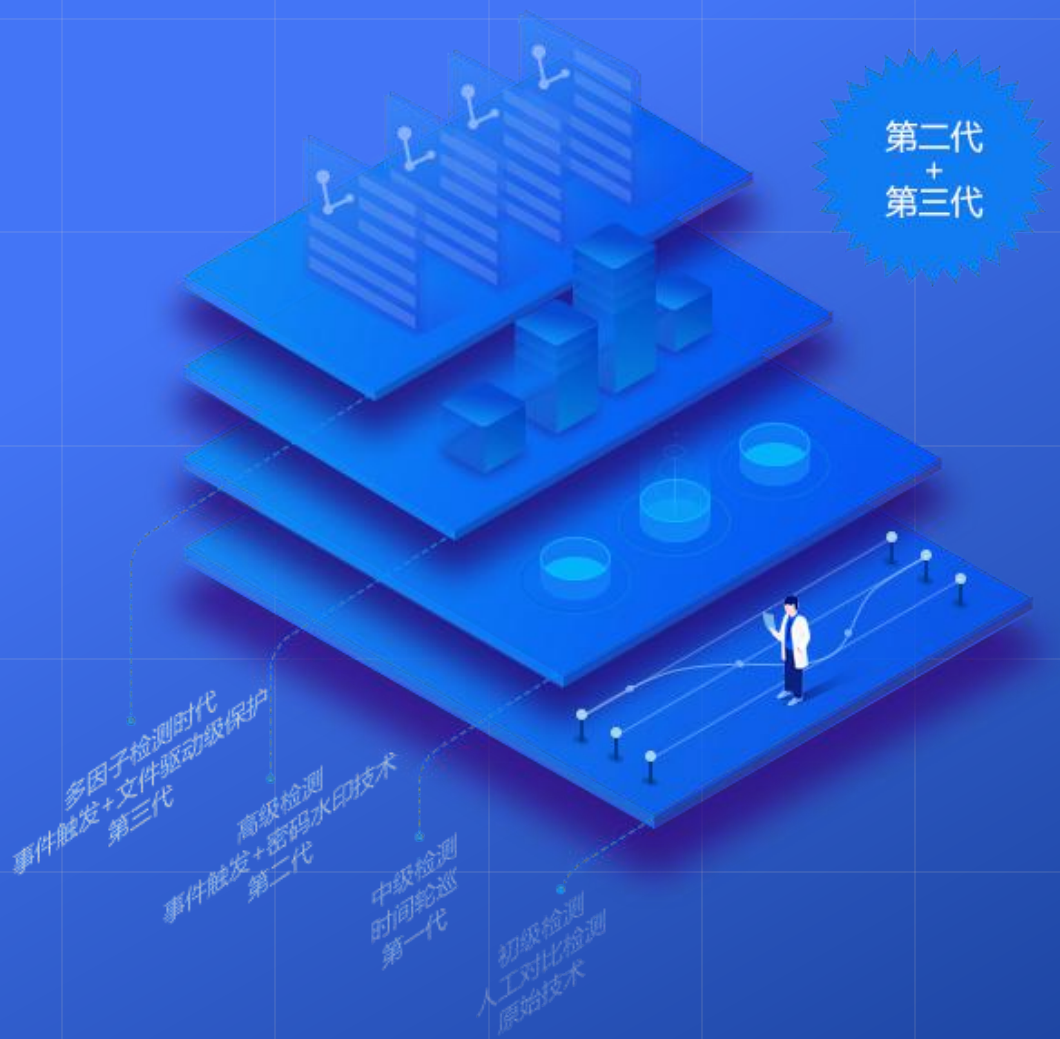
Web应用安全云服务

云磐通过网络层过滤和主机层应用自保护（RASP）相结合的技术，既能够过滤传统常见的攻击又可以对异常变形和未知漏洞的高级攻击进行识别，达到双层纵深防御的效果。

- 集中管理网站和WAF防护节点
- 通过平台设置各个防护节点安全策略，并下发至防护节点
- 以可视化的形式统计网站的安全状态，展现网站的风险和威胁
- 集中管理网站和WAF防护节点



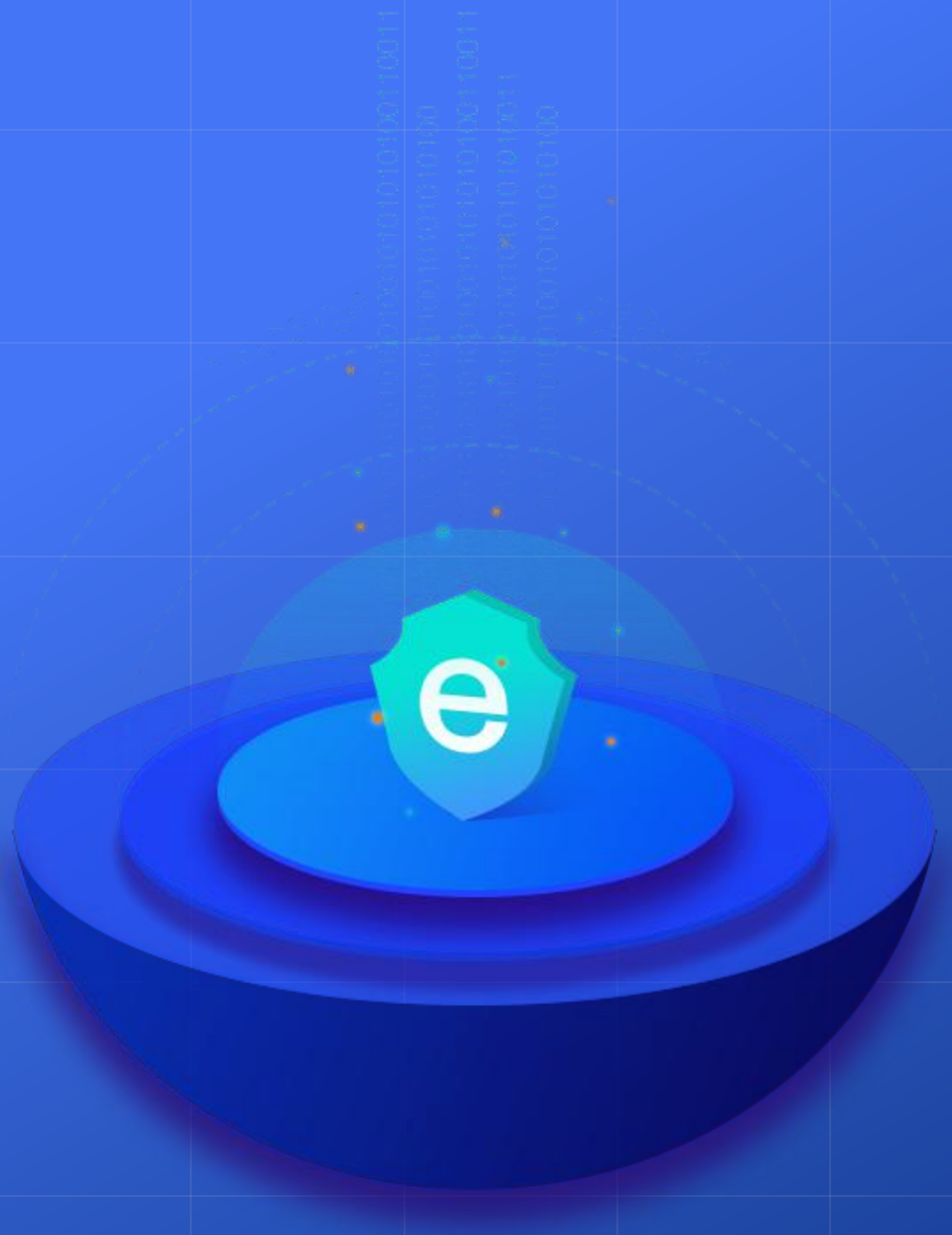
云磐安全服务体系



网页防篡改云服务

云磐采用第二代密码水印技术+第三代系统驱动级文件保护技术双结合，对网站安全进行双重防护，具有响应速度快、判断准确、资源暂用少及部署灵活等特点。

- 基于内核驱动防护技术，支持单独文件、文件夹及多级文件夹目录内容篡改保护
- 水印技术阻止被篡改网页流出，并自动恢复被篡改文件
- 支持断线状态下阻止篡改内容流出，返回篡改提示页面
- 完全防护技术，支持大规模连续篡改攻击防护



抗DDoS云服务

云磐提供了高效流量清洗中心，针对从网络层到应用层的攻击流量进行精确清洗。目前可清洗的流量峰值超过500Gbps。采用即用即开的机制，通过敏锐流量监测机制来弹性判断用户是否需要开启抗D服务。

- 快速感知，弹性控制，可快速适应不同流量的攻击
- 全面抵抗CC攻击以及各种纯流量攻击
- 专家全程参与防御，协助做出最正确的响应措施
- 能力强劲，可清洗的流量峰值超过500Gbps

云磐SECaaS解决方案

7*24小时安全专家服务

事前

风险评估

安全技术团队进行全面性
安全监测与加固服务

- 安全监测服务
- 安全加固服务
- 安全培训服务

安全监测及加固
事前发现风险

事中

定期巡查

安全技术团队定期协助
用户进行日常监控与巡查

- 告警日志分析
- 安全规则调整
- 定期安全报告

7*24小时云安全防护管理
事中常态化监控

事后

应急响应

安全技术团队1小时内
协助用户进行应急响应

- 安全事件分析
- 安全事件取证
- 安全事件溯源

7*24小时应急响应
事后取证及溯源

云磐SECaaS解决方案其他优势说明

费用

更少的采购费用支出

部署

更便捷的部署和配置

迭代

高效的产品迭代更新

补丁

持续的漏洞补丁更新

攻击

持续的攻击定义更新

规则

持续的安全规则更新

知识库

更全面的知识库信息

服务

专业团队全天候服务

03

安全狗与您携手面对

THREE

安全狗公司简介

安全狗
忠诚守护 值得信赖

基于智能驱动的新一代云安全公司

- 厦门服云信息科技有限公司（品牌名：“安全狗”）于2013年从美亚柏科（国内知名的安全上市公司）孵化，从成立开始就一直致力于主机安全产品的研发；
- 公司于2014年正式进军**云计算安全领域**，拓展云计算安全产品方面的研发，目前是国内领先的**云安全服务与解决方案提供商**；
- 公司多次入选国内网络安全**前50强**企业；并且成为国家应急响应中心CNCERT、国家网络安全与通报中心、国家信息安全漏洞库CNNVD、国家信息安全漏洞共享平台CNVD等**国家级单位的技术支撑单位。**

安全狗“春暖计划”

新型冠状病毒肺炎疫情发生以来，社会各界普遍响应，各行各业都以自己的方式支援武汉、支援疫情抗争一线。

在重大疫情面前，医疗战线的工作者都在不眠不休地与时间赛跑、与病毒赛跑，在努力打赢这场疫情防御之战。与此同时，国外APT组织对我国医疗系统的攻击、以疫情有关的名义传播的病毒和木马，这些事件无不提醒我们，医疗战线绝不是当前**“战疫”行动的唯一战场。**

目前网络安全行业已经普遍地动员起来，身体力行参与到“战疫”行动中。作为以**“忠诚守护 值得信赖”**为信条的安全企业，安全狗成立了专项工作小组，发布并执行了**“春暖计划”**，力图为严峻的“抗疫”形势带来一些暖意，帮助各重点单位应对特殊时期的网络安全风险。

安全狗“春暖计划”

个人角度，我们整理了一份注意清单：

·及时备份重要数据

·禁止将敏感重要的数据存储在网盘上

·安装杀毒软件并保持在线更新

·接收邮件时应注意发送者的邮箱，凡是要求点击链接的，都要十分小心

·谨防仿冒正规办公软件的恶意程序，尽量从正规应用市场下载办公软件，安装时需要对申请root权限及额外权限的应用警惕

·不接入不明及免密的公共WiFi热点，以免造成个人信息泄露

·避免公司内部数据与个人数据混用，尽可能选择安全的办公软件解决方案，访问公司内部数据需要开启身份认证

安全狗“春暖计划”

医疗行业

我们承诺，为医疗行业提供如下的免费安全产品和服务支撑

①在获得授权的前提下，为用户单位提供网站安全监测和渗透测试服务，找出当前系统存在的安全薄弱环节，并提供系统加固、修复的建议

②为用户单位提供全套云安全SAAS产品，包含：

- 主机安全防护（云眼SAAS版）
- 网站安全防护（云御SAAS版）
- 网页防篡改（云固SAAS版）
- 安全大数据分析及态势感知（啸天SAAS版）
- 网站安全监测及通报预警（海青SAAS版）
- 漏洞补丁管理（云网SAAS版）
- 安全专家值守

安全狗“春暖计划”

政务云、政府和教育信息平台

当前，很多与疫情防治有关的信息化平台都运行在政务云上，确保这些系统的正常安全运转已经成为了当前网络安全保障工作的核心之一。我们承诺，将继续为这些承载疫情防治关键信息系统的政务云平台，提供快速、高效的各类安全保障。

我们承诺，为涉及到在线教育和各类重要在线政务办理的政府和教育信息平台提供如下的免费安全产品和服务支撑

①为用户单位部署匹配场景的云安全SAAS产品，如云主机安全、web安全、补丁管理、安全大数据态势感知等

②必要时提供专家人工服务

安全狗“春暖计划”

各大云平台上的SAAS服务类型企业

当前众多线上信息系统的建设离不开云平台的支持和基础作用，截至目前，安全狗已经与各大云平台联合行动，为该云平台上的SAAS服务类型的企业提供有关的免费安全产品和服务

我们承诺，将为所合作的云平台上、符合条件的SAAS服务类型企业提供免费的云安全SAAS产品，包括：

·主机安全防护（云眼SAAS版）

·网站安全防护（云御SAAS版）

·网页防篡改（云固SAAS版）

·安全大数据分析及态势感知（啸天SAAS版）

·网站安全监测及通报预警（海青SAAS版）

·漏洞补丁管理（云网SAAS版）

·安全专家值守

安全狗“春暖计划”

各类线上平台

疫情让人们无法出门，很多需求需要靠在线平台来满足，在线办公、在线教育、在线电商（生鲜采购和外卖等）为人们提供了重要的生活服务支撑。

我们承诺，为上述在线平台提供如下的免费安全产品和服务支撑

·帮助用户监测网站异常动态、及时修补漏洞，避免不法分子破坏、肃清威胁

·为用户单位部署匹配场景的云安全SAAS产品，如云主机安全、web安全、补丁管理、安全大数据态势感知等

·必要时提供专家人工服务

总结

衷心祝愿所有奋斗在抗疫一线的工作人员——包括医生、护士、民警、社区……还有网络安全工作者——平安归来！

感谢所有无私付出的人们，祝愿疫情早日结束，大家可以甩掉口罩，畅快呼吸！

联系方式

安全狗
忠诚守护 值得信赖

谢谢！

忠诚守护 值得信赖

厦门服云信息科技有限公司
400 1000 221 www.safedog.cn