网宿科技 WANGSU.COM | 网宿安全 WANGSU SECURITY

2023年度
互联网安全报告
「体系化主动安全」建设指南

智 能 边 缘 安 全 领 导 者

目录 CONTENTS

引言

2023年全球网络威胁形式依然十分严峻。与往年相比，2023年曝光的通用安全漏洞数量再创新高，其中包含了大量遭黑客积极利用的高风险漏洞。网络黑灰产团伙仍十分的活跃，DDoS攻击、Web应用攻击、API攻击、网络爬虫、业务欺诈等几种活跃性攻击的趋势有增无减。屡见不鲜的针对于高价值企业的定向攻击勒索、数据窃取等事件，则将网络安全风险的严峻程度推向了新的高度。

对企业来说，新的变化往往也意味着引入新的风险。数字化转型的进一步深入、IT基础设施的升级迭代、业务全球化过程中办公模式的转变等等也带来了不断变化增长的风险暴露面，数据的流向更加不可捉摸；攻击者也在升级，瞄准业务层、身份层的攻击让传统基于特征的防御模式已难以应对；生成式AI技术的发展也在推动着攻击技术的快速进步，这让网络防御更加充满了不确定性和复杂性。为此，企业在构建安全体系时不仅要充分考虑防御的全面性，尽量去覆盖保护所有潜在的网络攻击面，也要考虑如何去构建更加积极主动的安全防御能力，才能够适应不断变化升级的网络威胁。

传统安全建设思路是通过堆叠各种不同保护层级与防御形态的安全产品去构建防御体系，为了管理这些分散安全能力，安全人员需要在多个安全产品控制台之间去切换操作，这对安全效率是一种严重阻碍。为了解决这一问题并让安全产品之间能够协同运作、形成主动安全防御能力，安全管理人员试图再引入具备统一集中管理与安全能力编排的工具以整合企业分散安全能力，但是由于缺乏安全专家、不同供应商的产品异构性、接口封闭等因素，这些单点安全能力往往很难能协同运作。

继续基于传统的烟囱式安全能力简单叠加模式进行防御，已难以满足当前企业对于追求安全效果的期望；经济环境的不确定性也使得企业需要在收紧支出的同时，重新评估当前繁杂的安全工具对IT支出的占用。安全负责人需要寻找具备真正的“体系化主动安全能力”且兼具经济性的安全解决方案。“体系化”要包含防御的全面性、统一集中管理、灵活场景覆盖等构建原则；“主动性”则是要求具备对于未知风险的防御能力，能够及时自动的对网络威胁进行响应处置。

本次报告也将围绕“体系化主动安全能力建设”这一主题，基于网宿安全平台提供的攻防数据、企业侧的安保实践，以及全球网络安全趋势的分析预测，帮助广大企业用户建立“体系化主动安全”防御机制。

第一章 威胁泛化：Web安全态势分析与应对指南

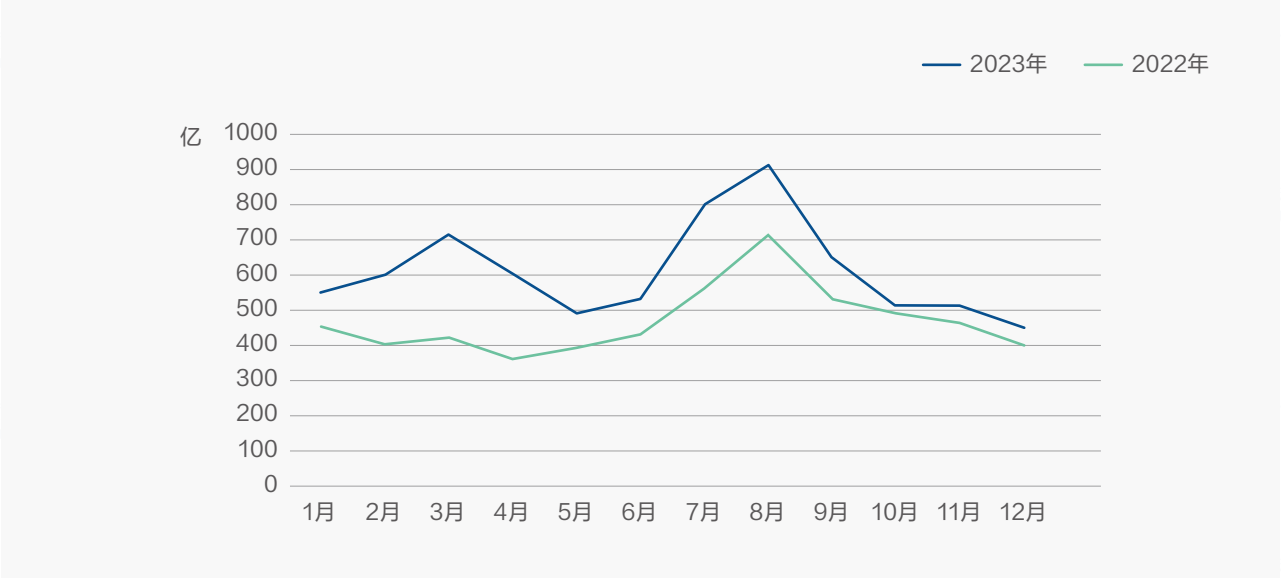
本章节通过对2023年网宿安全平台检测到的网络攻击行为与事件进行统计分析，结合企业当前数字化和云化进程、生成式AI等新技术的兴起，探讨传统Web安全解决方案暴露出的瓶颈，及以一体化Web应用和API保护（WAAP）应对新威胁形势的必要性。

章节后半部分，将基于网宿安全实践，提供一体化WAAP建设指南，帮助企业通过统一管理攻击面和纵深防御策略，提升整体Web安全防护能力。

1.1. 2023年Web威胁态势分析

1.1.1. 全球Web应用程序攻击超7千亿次，持续快速增长

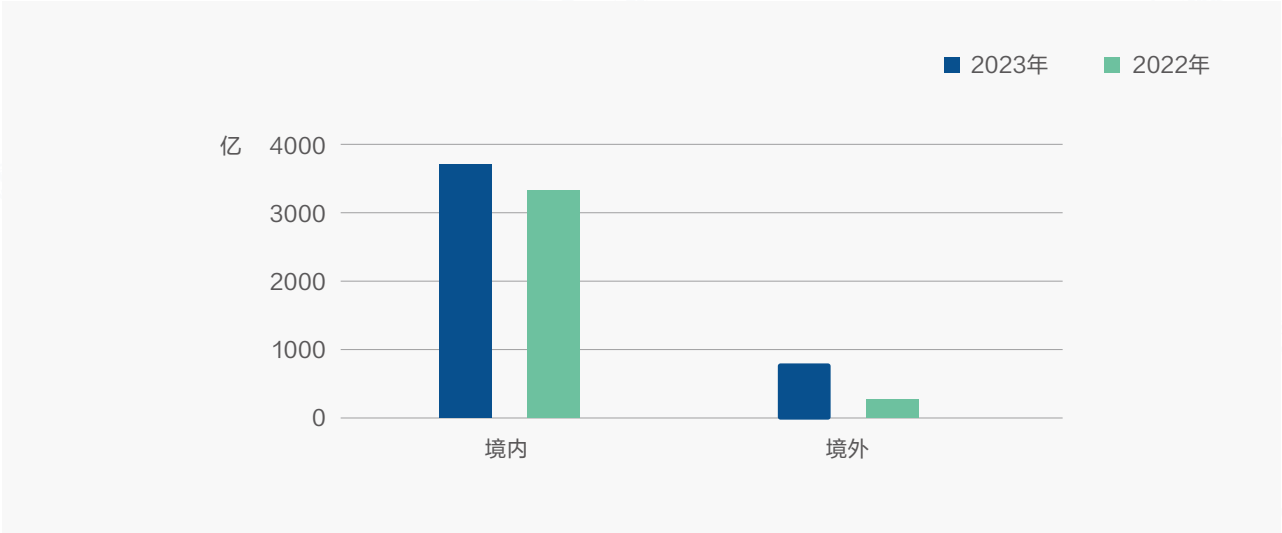
从网宿安全平台代理的所有Web应用程序流量来看，2023年被检测到的攻击请求数量为7309亿，占比达到20%，相比2022年的 5602亿次增加了30%。通过下图2023年和2022年攻击趋势对比可以看出，全球Web应用程序攻击仍在持续增长。



我们发现增长主要源于以下几方面：

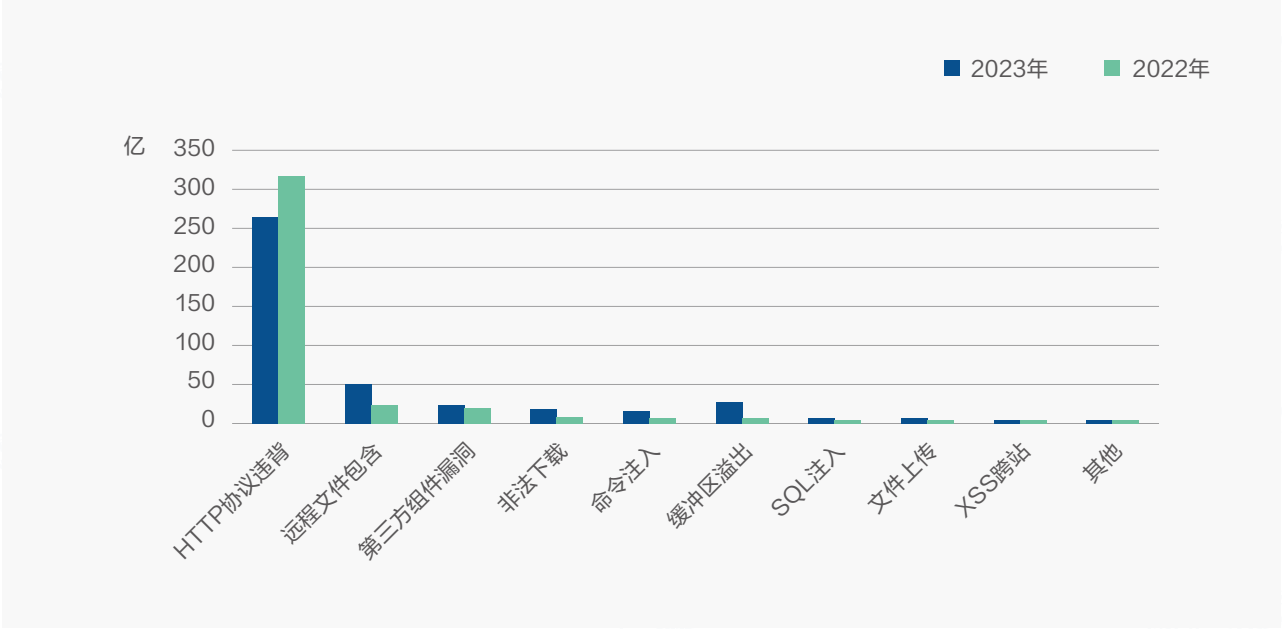
- **针对境外目标的DDoS攻击在2023年增长了近220%**

2023年，全球应用层DDoS攻击次数达到4500亿次，同比增长26%。下图表明，2023年针对境外目标的攻击增长明显高于境内。针对境外目标的攻击在2023年增长了近220%，境外攻击为总增长贡献了90%以上的份额。我们分析推测这一趋势与中国企业加速“走出去”战略以及欧洲地缘政治冲突的激增密切相关。



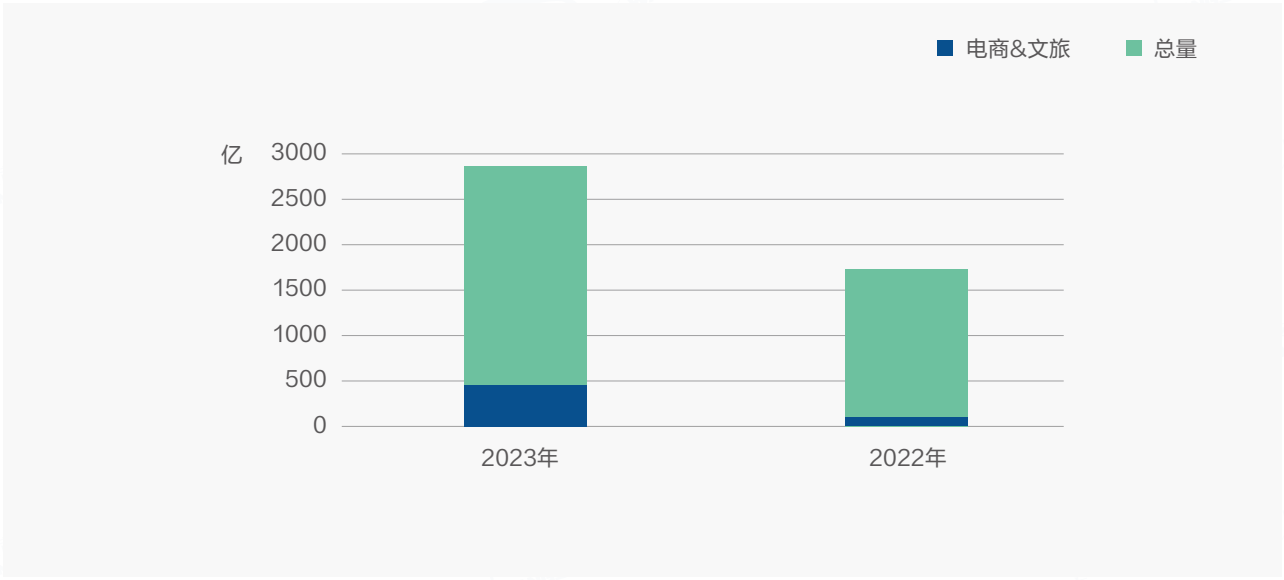
自动化攻击进一步普及，促使漏洞利用攻击增长8%

根据网宿安全平台数据统计，2023年共检测到416亿次Web应用漏洞利用攻击，同比2022年增长8%。其中HTTP协议违背依旧排名第一，但相对2022年下降了3.8%，从这个数字变化上可以猜测整体攻击高度的变化，攻击逐步摆脱“一眼看破”的低级攻击，更多地利用自动化工具甚至生成式AI技术构造更为聪明的攻击，同时也带来了攻击数量增长。



直播电商兴起、文旅行业复苏，恶意Bot请求增长172%

后疫情时代，人们使用在线购物的比重持续增加，也衍生了直播电商等新兴购物形式，同时压抑已久的线下演艺活动得到释放。电商、演艺行业在线业务流量增加也伴随了大量爬虫、欺诈流量增加。2023年网宿安全平台检测到的电商、文旅行业恶意Bot请求数达到462亿，占全平台Bot请求数比例为22%，相比2022年的170亿、10%分别增长172%、120%。

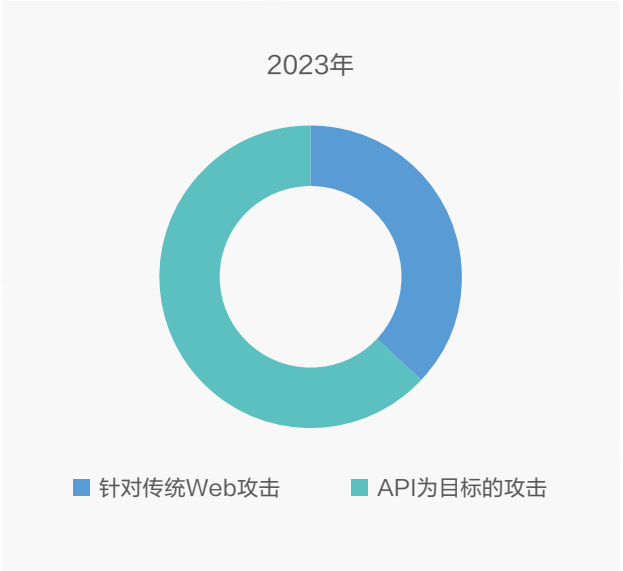


1.1.2. 生成式AI威胁崛起，Web安全威胁多维度升高

数字化时代，业务接入渠道日益丰富、API大量应用，导致Web应用风险暴露面显著扩大，Web安全威胁多维度升高，已成为显而易见的事实。2023年，以下风险变化趋势值得关注：

- **API攻击占比继续走高，多维度应用安全风险加剧，数据安全问题凸显**

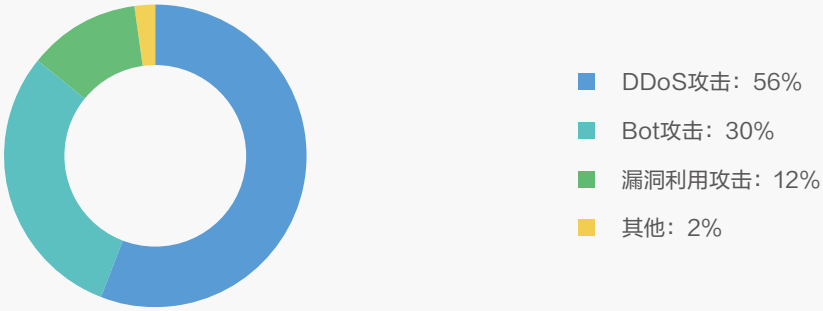
2022年，网宿安全平台数据针对API的攻击占比首次突破50%，达到58.4%，2023年进一步上升到了63%。进一步分析，我们发现这一数字正是Web安全风险多维度上升的直观体现。



一方面，自动化攻击是针对API攻击的最常用手段，究其原因是API承载着关键数据和业务，利用僵尸网络针对API发起DDoS攻击能直中要害造成核心业务停摆，利用自动化Bots针对API发起Bot攻击，能够快速获取高价值数据，或通过欺诈获益。

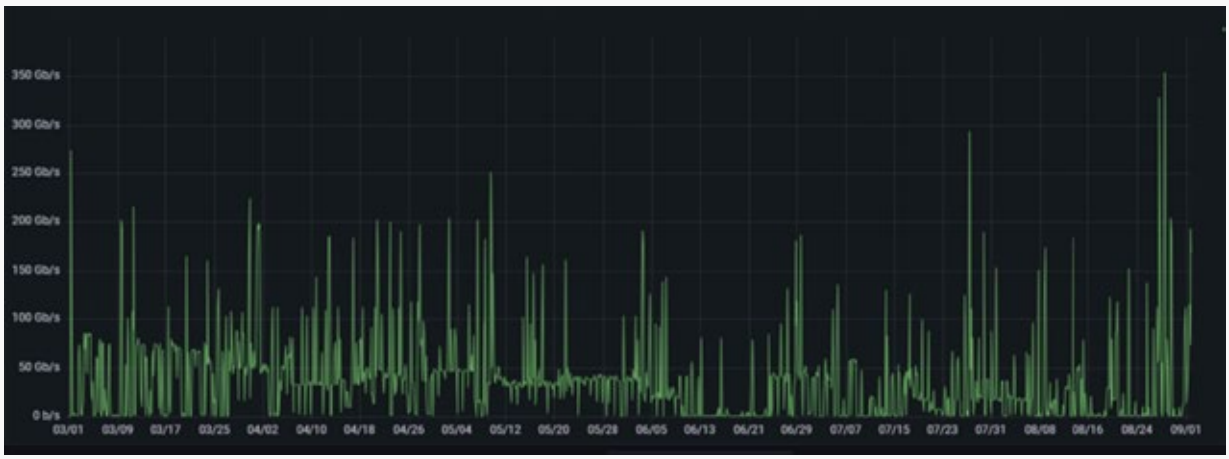
另一方面，利用API漏洞进一步实施勒索等攻击，导致数据泄露等严重后果，给企业带来巨大威胁和损失。例如：2023年5月MOVEit 0day漏洞被Cl0p组织利用入侵并进行勒索攻击，超过9300万人的个人数据被泄露，影响2706个组织。

网宿安全平台数据显示，针对API的攻击类型占比如下：

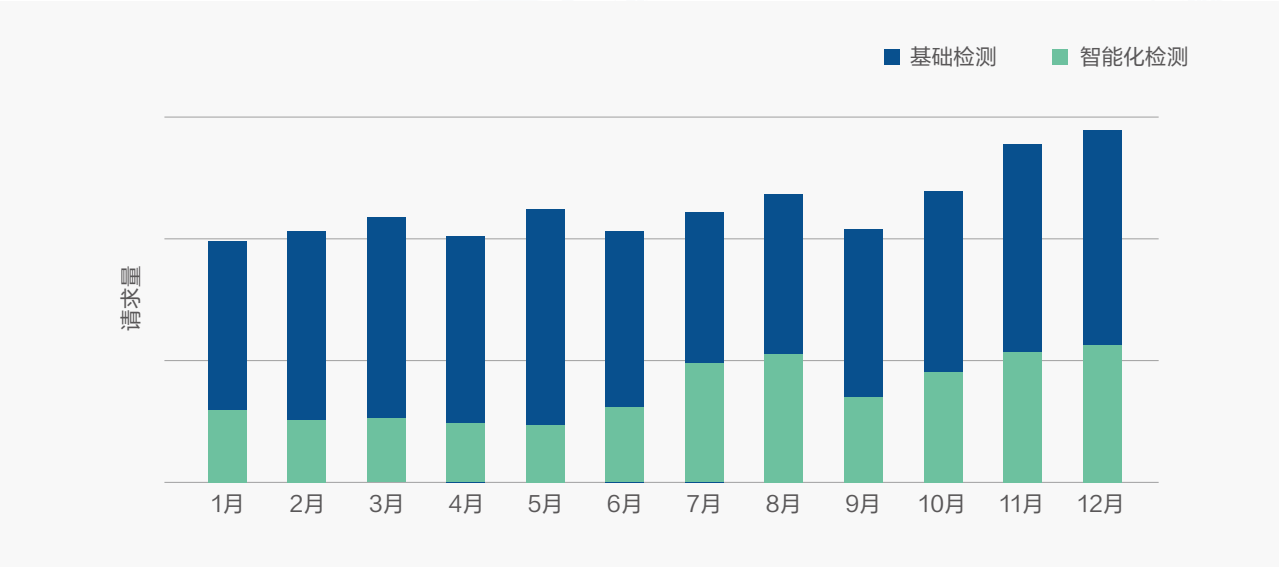


攻击手段更隐蔽、更智能化

DDoS攻击方面，网宿安全演武实验室研究发现，攻击者的攻击方式变得更为精巧，攻击目标的业务特点，在业务低峰期仅发起较低的攻击量级，在高峰期突然提高攻击量级对业务造成更大冲击，较强的随机性使企业安全团队难以及时响应和对抗，同时攻击者也能以最低成本最大化攻击收益。



Bot攻击方面，随着生成式AI的爆发式兴起，自动化攻击的手段越来越隐蔽。为此我们在2023年优化了Bot智能识别能力，进一步融合基础特征、访问行为、情报、交互检测等更多维度、基于AI技术落地识别模型，从目前深受Bot困扰的行业来看，Bot智能识别能力已经贡献了超40%的Bot识别率，而且这一比例还在上升。



新型攻击威胁层出不穷

继基于HTTP/2 Rapid Rest漏洞的严重HTTP DDoS攻击之后，我们在2023年发现又一基于HTTP/2 Continuation Flood的新型威胁。攻击者利用这一攻击原理，可以轻松发起大规模的DDoS攻击。其攻击峰值RPS（每秒请求数）相比传统HTTP Flood可实现一个数量级突破，从千万级到亿级。

*【*HTTP/2 Continuation Flood*】*

HTTP/2 Continuation Flood 漏洞的目标是未正确处理 HEADERS 和多个 CONTINUATION 帧的 HTTP/2 协议实现。威胁行为者发送一系列不带 END_HEADERS 标志的 CONTINUATION 帧，导致潜在的服务器问题，例如内存不足崩溃或 CPU 耗尽。HTTP/2 Continuation Flood 可以做到通过仅允许单台机器就能够破坏使用 HTTP/2 的网站和 API，但由于 HTTP 访问日志中没有可见的请求，这种攻击难以被发现。

生成式AI威胁不容忽视

2023年生成式AI技术取得了显著进步，同许多技术创新一样，生成式AI在提升效率的同时，也会成为攻击者武器库的一部分。在Web安全领域，我们发现生成式AI能通过以下方式助长攻击威胁：

1）让现有攻击更隐蔽，逃避检测

网宿安全演武实验室研究发现，使用生成式AI能够比常见的FUZZ工具生成语法和逻辑结构上更加复杂和隐蔽的攻击Payload，一部分已经能够绕过当前针对FUZZ工具的检测手段。类似地，生成式对抗网络(GANs)可以用来生成复杂的恶意软件变种，使得传统的基于签名的恶意软件检测方法失效。

2）自动化攻击生成

通过训练生成式AI模型理解和生成攻击代码，已经能够自动生成针对特定应用软件的攻击代码。例如，使用Transformer等自然语言处理技术，可以对已知的攻击策略和漏洞信息进行学习，进而生成专门针对新发现的漏洞的攻击代码。

3）渗透测试自动化

通过AI可以将渗透测试过程部分环节自动化，并被训练用以模拟攻击者的行为和策略，更高效地发现并利用系统漏洞。

4）增强攻击的持续对抗能力

经过特定领域训练过的大模型可以生成多阶段攻击脚本，使得攻击能够在被发现和部分阻断后继续进行，增加了防守方的应对难度。

1.1.3. 企业传统Web防护体系挑战严峻

企业安全团队基于现有的传统防护体系应对日益复杂且泛化的Web安全威胁时面临严峻挑战。传统防护体系存在的诸多问题使其难以全面有效地应对现代Web安全威胁。

传统WAF的核心问题包括：

难以全面防御日益复杂的攻击

传统WAF主要依赖预定义的规则和签名来检测威胁，面对攻击者发起0day漏洞攻击、或使用自动化工具发起不携带特征的数据爬取、API滥用等新型攻击时，则束手无策。

安全团队负载高，安全事件响应速度慢

安全团队本就需要处理大量安全事件和告警，而传统WAF规则需要不断更新维护和误报处理的重复性工作进一步加重了工作负担，导致真正发生严重安全事件时无法快速响应。

难以适应云原生架构和Devops模式下Web应用快速迭代

企业越来越多地采用混合云和多云部署，传统WAF在多样化环境中的部署和管理变得复杂，难以提供一致的安全保护。另外，现代应用基于Devops模式快速迭代开发，传统WAF难以快速适应应用的变化和扩展，影响了安全防护的有效性。

缺乏全面的威胁情报，无法全面感知风险态势和及时防御新兴威胁

对于Bot、API攻击等以数据为核心载体和目标的新型攻击，需要通过大数据和AI技术构建智能化的动态对抗能力。而威胁情报则是构建此能力的核心基础数据之一，传统WAF存在数据孤岛、或与新型攻击相关的先进情报（如：IP信誉库、指纹库）缺乏整合，对于恶意Bot流量、API滥用导致数据泄露等风险态势无法及时感知并快速防御。

企业安全团队需要一个全面和先进的防护体系来解决上述问题，Gartner提出的WAAP（Web应用和API保护）正是为此而设计，企业以WAAP核心能力为底座，结合安全风险管理的实际诉求，能够建立适应现代Web威胁环境的下一代Web安全体系。

1.2. Web安全体系建设指南

1.2.1. 从传统WAF向WAAP防护体系升级

WAAP（Web Application and API Protection，Web应用和API保护）是综合性的安全解决方案，旨在保护Web应用和API免受各种网络攻击。WAAP可以视为是传统Web应用防火墙（WAF）的升级方案，通过集成多种安全功能，提供全面的威胁检测和防御体系。主要功能包括Web应用防火墙、DDoS防护、Bot管理、API安全、威胁情报和自动化响应等。

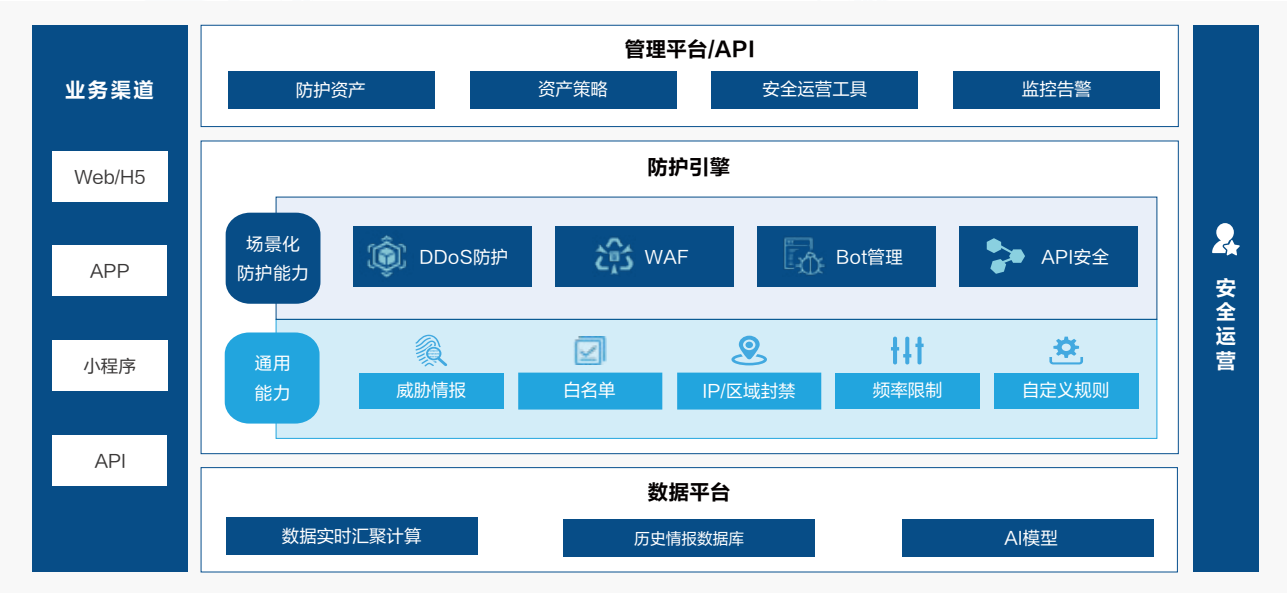
WAAP和WAF相比，关键区别有：

	WAF	WAAP
防护对象	主要防护传统Web应用	在防护Web应用之外还扩展了对API的防护
防护范围	主要防护SQL注入、跨站脚本等常见OWASP Top10威胁	在WAF基础上还集成了对于DDoS、Bot和API攻击的防护
核心技术	主要依赖预定义的规则和签名	在WAF基础上重点采用了AI和行为分析技术，通过访问流量、威胁情报等数据驱动形成对于新型复杂攻击的自动化防护和响应能力
适用场景	适用于静态或变化较小的应用环境，且只需要基本防护的企业	适用于动态和多云部署的现代应用环境，且需要全面安全防护以应对复杂威胁的企业

1.2.2. WAAP防护体系架构实施建议

对于已进入数字化进程的企业，网宿建议尽早通过建设WAAP防护体系架构，并结合自身安全风险管理的实际诉求，构建符合现代Web安全威胁态势的整体安全方案。

WAAP防护架构参考下图：



具体建设落地方式建议如下：

- **顶层设计**

应从顶层设计角度出发，规划建设统一的WAAP防护平台，包括接入所有业务渠道、整合为一的防护引擎、底层统一数据平台，再通过一个管理平台将以上能力串联并呈现，帮助安全团队真正实现全业务、全架构的统一安全管理。

另外，在设计时就应考虑将WAAP防护架构纳入企业安全风险管理体系，实现安全风险全流程闭环。例如：与资产和攻击面盘点结合，保证面向公众的Web应用都处于WAAP保护范围；与SOC或SIEM集成，充分利用WAAP丰富的防护能力和数据进行高效的安全事前事中处置和事后修复。

全业务渠道接入

安全风险本质上来自于业务，因此WAAP防护架构需要覆盖几乎所有业务接入渠道，尤其是风险敞口最大的面向公众开放的互联网业务，包括Web/H5网站、APP/小程序、API等。需要特别注意的是，虽然API不是一个独立的业务渠道，但由于其有别于传统Web应用的技术和安全风险属性，也需要建设API资产发现和接入等相关能力，将API作为其中一个安全管理对象。

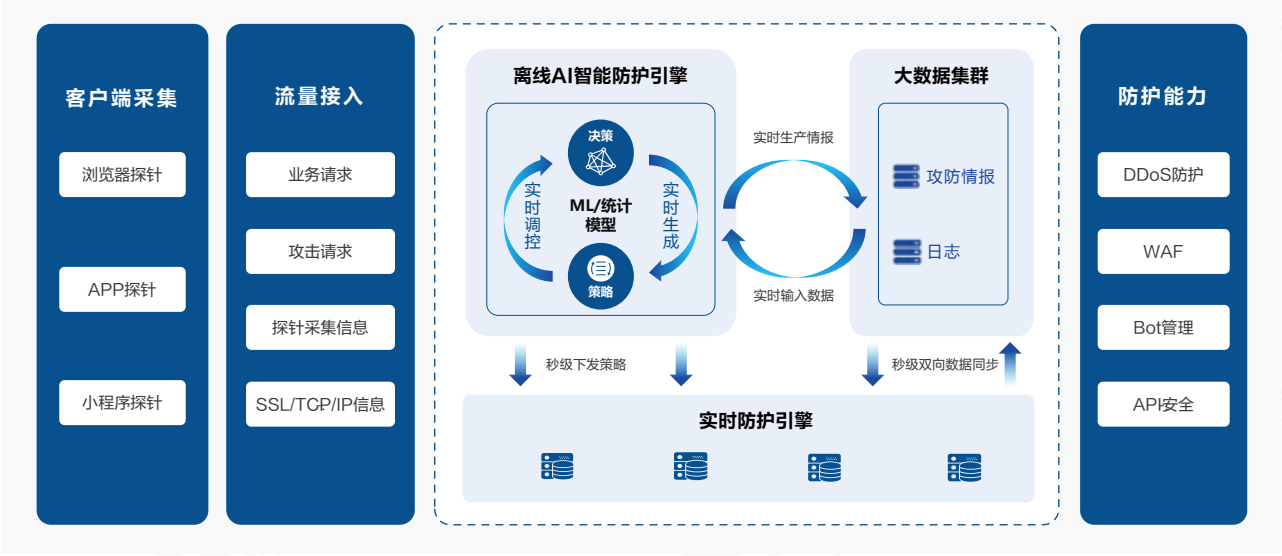
统一管理平台和API

统一管理平台，能够让安全团队工作效率最大化，从而获得最大的安全投入回报。具体而言，通过统一的管理界面，安全团队可以一致地管理所有防护资产、安全策略和安全事件，通过统一的API，可以通过Devops模式将应用开发和安全性自动化管理起来，既减少人力投入，又增强了WAAP防护动态适应应用变化的能力。

数据驱动和AI应用

建设统一数据通道和平台，并将AI技术实际应用到防护场景中，是不可或缺的投入。WAAP在应对新型复杂攻击时，与WAF技术上最核心的区别就在于对数据的有效整合和应用。

核心防护能力



WAAP核心防护能力建设时，需要包含上图中的四个方面：

1. 客户端采集	2. 流量接入	3. 实时和离线双防护引擎	4. 防护能力
爬虫、API滥用等现代攻击大量使用自动化客户端工具发起，因此通过客户端植入探针采集客户端环境和行为等信息用于安全监测是有效对抗此类攻击的必要条件。探针的具体实现方式有浏览器页面嵌入JS、APP或小程序嵌入SDK等	业务和攻击流量中的HTTP请求、探针采集信息、SSL/TCP/IP信息统一通过流量接入WAAP防护引擎中，用于安全检测。常见的接入方式是通过SaaS化服务反向代理用户访问流量	简单的攻击通过一些明确特征规则在实时防护引擎中直接检测并拦截，隐蔽性强的复杂攻击则需要把采集到的所有数据经过离线AI智能防护引擎检测识别，再把最终阻断攻击的指令下发给实时防护引擎，从而覆盖从简单到复杂的各类攻击	基于充分协同的客户端数据采集、流量接入、防护引擎，构建出WAAP的四大核心防护能力，即：DDoS防护、WAF、Bot管理和API安全

通过WAAP防护体系架构，企业可以获得：

1. 业务能够全面抵御DDoS、SQL注入、跨站脚本、恶意机器人和API滥用等核心安全威胁；
2. 对新型复杂攻击具备有效的自动化、智能化检测和响应能力；
3. 简化安全管理，减少误漏报处理人力投入，更高效处理真实安全事件，提升安全团队效率；
4. 在多云和混合云环境中提供一致的安全保护，与Devops集成，保障应用在快速变化中的安全性。

1.2.3. WAAP防护体系实践案例

网宿安全基于WAAP和风险管理理念构建的全站防护解决方案，已在多个行业和场景中应用落地，成效显著。典型场景列举如下。

场景1：某SaaS服务商全球业务统一防护

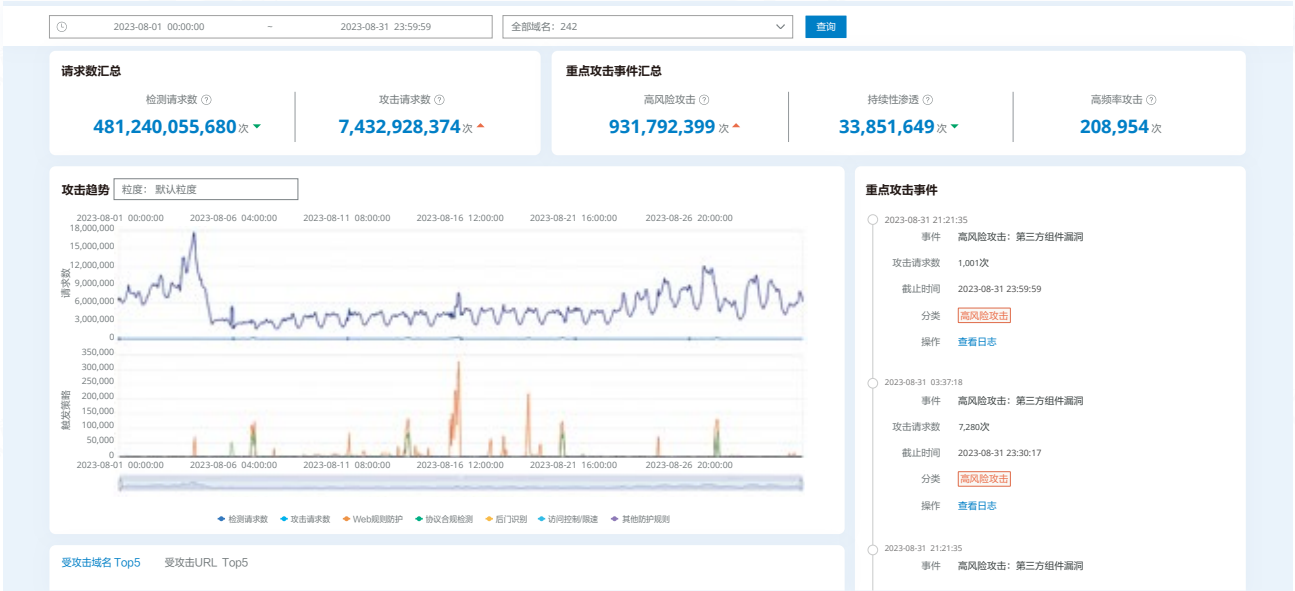
某SaaS服务商业务分布全球，面向不同国家分别构建不同网站，在安全上主要存在几方面的挑战：

1. 使用了不同国家的云基础设施，多云管理困难，运维和安全人员工作量大；
2. 业务面临着DDoS、Web攻击、爬虫等多方面的威胁，原先使用多个产品影响用户访问性能；
3. DDoS攻击、爬虫经常出现漏过回源，频繁调整策略跟不上攻击变化，还会引入误拦截，安全团队疲于被动应对。

网宿WAAP全站防护解决方案：

1. 将多个云上的网站域名通过CNAME统一接入到全站防护平台，统一进行资产和安全管理；
2.全站防护所有防护模块均集成在CDN边缘节点，仅需一次解包即可实现全面检测，业务接入后用户整体访问速度有所提升；
3.网宿全站防护全面应用AI技术，提供DDoS AI智能防护、WAF规则自学习适应、Bot智能检测等能力，大大降低误漏报，在此基础上提供丰富的告警维度，使安全团队主要关注真实告警和处置决策。

使用WAAP方案后，平均每个月低于百万级DDoS攻击十余次，拦截Web攻击和爬虫超过800万次，业务在线0中断；安全团队每月处理告警相比分别使用单一防护产品下降60%，告警通过统一的态势和策略页面分析处理，处理时效缩短50%以上。



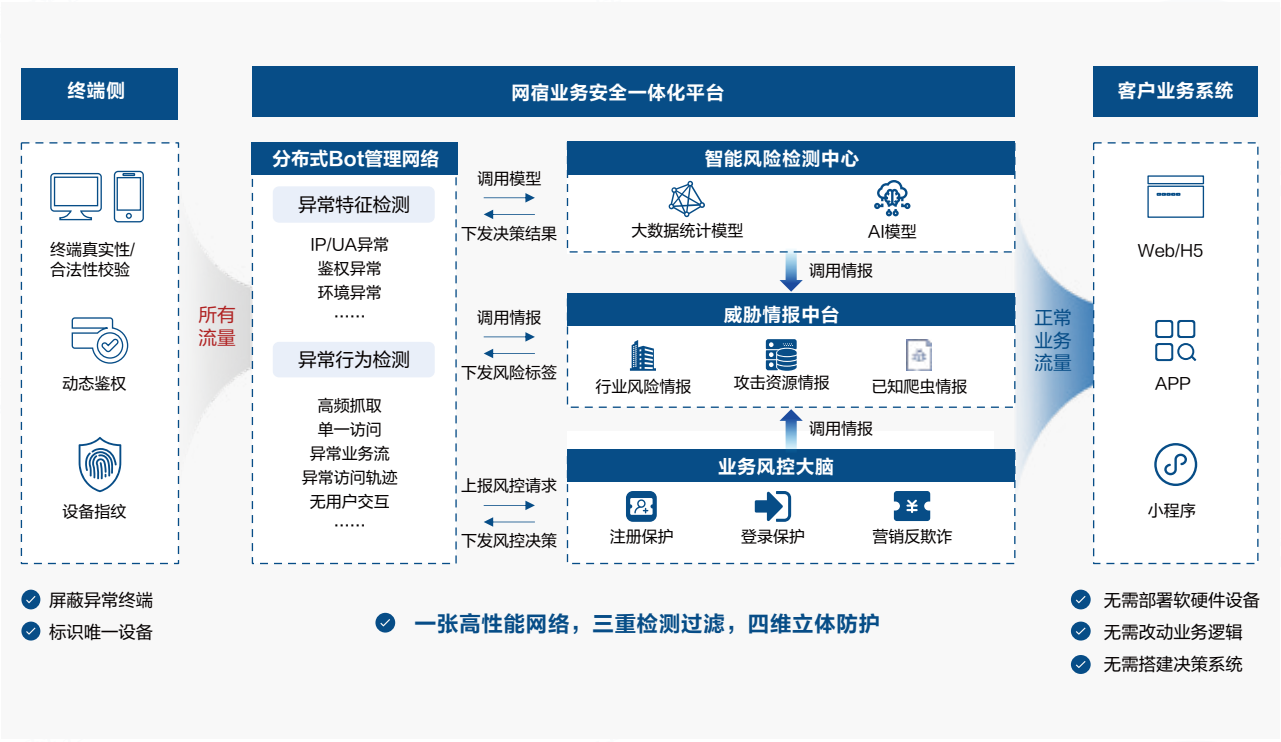
场景2：某美妆集团在线营销反薅羊毛

某知名国际美妆品牌自建电商渠道，通过丰富的会员营销活动吸引用户、促进回购、保持用户对品牌的忠诚度，开展营销活动时品牌IT和业务部门面临巨大挑战：

1. 抢购场景并发量大：高峰期下单、加购等接口访问量是日常的300多倍，导致服务器崩溃；
2. 黑灰产“薅完即走”，不会产生附加订单，营销活动ROI低；
3. 以js为主要技术手段的防Bot方案无法有效对抗高度拟人的薅羊毛行为，风控系统检测和运营的压力巨大。

网宿WAAP全站防护解决方案：

基于全站防护一体化平台，针对简单自动化工具、接口破解薅羊毛、真人欺诈进行分层治理。



使用WAAP方案后，成功保障30W QPS活动并发，在薅羊毛最猖獗的一次活动中，有接近95%的自动化工具请求由Bot管理网络自动成功化解，对于少量真人欺诈行为，通过风控大脑平均每次活动识别到1.2w+个可疑账号，业务部门对账号进行取消订单等处理，总体共计挽回数百万无效的营销支出。

第二章 重塑边界：办公网络安全态势分析与应对指南

2.1. 2023年企业办公网络威胁态势分析

在当今数字化高速发展的时代，企业办公网络宛如企业的中枢神经系统，承载着企业的关键数据、核心业务流程以及与外界交流合作的重要通道。然而，伴随着网络技术的日新月异，企业办公网络所面临的安全威胁也愈发复杂多变、严峻棘手。

2023年，对于众多企业而言，网络安全形势犹如风云变幻的战场，充满了未知与挑战。在众多的网络安全威胁中，勒索软件攻击和数据泄露无疑是最为主要且最受企业关注的两大核心问题。

勒索软件攻击，这种恶意且极具破坏力的手段，给企业带来了巨大的困扰和损失。攻击者利用先进的技术手段和精心设计的策略，入侵企业的网络系统，对重要数据进行加密锁定，并以此要挟企业支付高额赎金。这种攻击不仅直接导致企业业务的停滞，还让企业陷入两难的抉择：支付赎金可能助长攻击者的气焰，同时也无法确保数据能够完全恢复；不支付赎金，则可能面临数据永久丢失、业务长期瘫痪的风险。

而数据泄露更是企业的“心腹大患”。企业在日常运营中积累了大量的敏感信息，包括客户的个人数据、商业机密、财务信息等，一旦这些数据因网络安全漏洞而被泄露，将引发一系列连锁反应。客户的信任度会急剧下降，企业的声誉遭受重创，可能面临法律诉讼和监管部门的严厉处罚，同时还会为竞争对手提供可乘之机，严重影响企业在市场中的竞争地位。

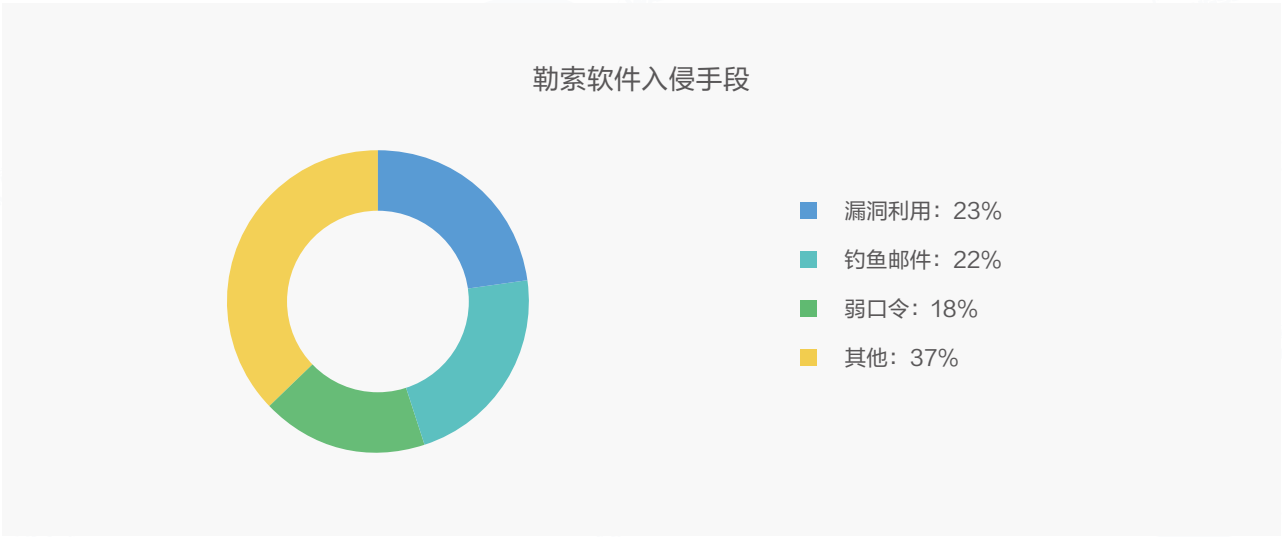
网络安全威胁已不再是孤立的技术问题，而是关乎企业生死存亡的战略问题。深入剖析和研究网络安全威胁的态势，尤其是勒索软件攻击和数据泄露这两个关键领域，对于企业制定切实有效的防御策略，保障企业的正常运营和稳健发展，具有至关重要的意义。

2.1.1. 勒索软件攻击事件翻倍增长

勒索软件是一种恶意软件，其运作方式极为恶劣且具有破坏性。勒索软件攻击在2023年仍然是企业面临的极为严峻的威胁之一。根据网宿安全演武实验室观察到的数据趋势，相较2022年，2023年企业办公网络遭受的勒索软件攻击事件增加了一倍以上。

- **攻击手段**

攻击者通常会利用各种手段，如网络钓鱼邮件、恶意软件下载链接，或者通过系统漏洞入侵企业的网络。一旦成功渗透，勒索软件会迅速在企业内部网络中传播，对大量的重要文件、数据库和业务系统进行加密锁定。这使得企业的正常业务运营瞬间陷入瘫痪，无法进行日常的工作流程，如文件查阅、业务处理等。更为糟糕的是，攻击者会向企业发出勒索要求，威胁企业支付高额赎金以获取解密密钥，恢复数据的访问权限。



网宿安全演武实验室基于对勒索软件入侵事件的分析发现，通过漏洞利用、钓鱼邮件、弱口令占据入侵攻击手段的六成以上，成为企业面临的主要网络威胁。同时，勒索软件对某些高危和超危等级的漏洞利用较为频繁，2023年有44个漏洞被全球勒索组织频繁利用，77%的常用漏洞类型主要为远程代码执行与权限提升漏洞，针对这两种漏洞类型的利用，一是让攻击者能够成功进入目标系统，二是能够获取对系统更高级别的控制权限，从而扩散攻击范围，其中，零日漏洞(0day)造成的影响最为严重。此外，2023年还出现了多种新型攻击手法，例如，深度学习和AI技术被用于生成更加精准的钓鱼邮件，提高了欺骗性。

攻击目标

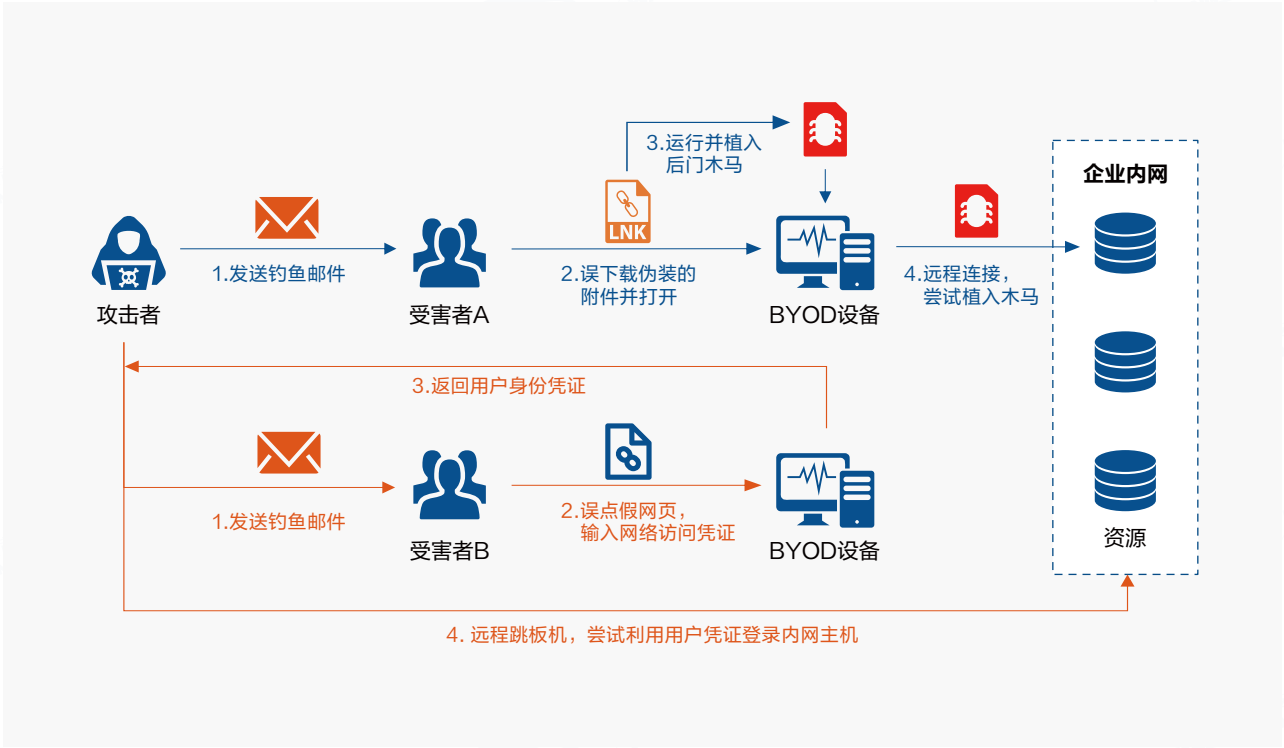
在攻击对象方面，约1/3的攻击事件主要瞄准了政府、金融、能源、医疗等机构，这些机构承载重要社会职能，所运营的行业信息系统有着大量数据资源，所以被作为实施攻击的“高价值”目标。而其余约2/3的攻击事件则是倾向于将目标扩展至那些对网络安全投入有限，但又拥有大量敏感数据的中腰部企业。

关键基础设施单位和重要行业通常是国家安全和社会运行的关键节点，包括能源、交通、金融、公共服务等领域。通过对网宿安全平台监测到的攻击事件中的目标企业和机构进行画像分析，发现这类企业和机构的安全防护本身较为严密，具备一定的抵御能力。这类企业和机构往往关注暴露面收敛、网络邮件钓鱼防护，并且每年花费2个月以上的时间用于投入钓鱼模拟、攻防演练的实战中。然而，攻击技术的不断提升，尤其是随着APT（高级持续性威胁）攻击，勒索软件可能会长时间潜伏在系统内部，搜集信息，寻找攻击时机。

与头部关键企业相比，中腰部企业往往因为资源有限，对安全投入不足，从而导致安全防护水平较低，容易成为攻击者的目标。这些企业可能包括中小型制造业、地方性金融机构、教育机构、零售业等，它们在安全措施、人才队伍、应急响应能力等方面存在不足。攻击者往往利用这些企业的安全漏洞进行入侵，而一旦遭受攻击，不仅可能导致企业自身运营受损，还可能波及到上下游供应链，影响更广泛的行业生态。

勒索软件攻击案例

以网宿安全演武实验室观察到的某个物流服务企业的攻击事件分析为例，该企业的供应商日常通过BYOD设备进行远程办公访问企业内网，某天收到伪装成该企业发送的“办公系统紧急升级”钓鱼邮件，其点击了假网站链接并输入了企业分配的网络访问凭证进行“身份验证”，从而毫无察觉地被窃取了内网账户登录信息，该用户凭证因在异地首次通过新设备和新IP尝试登陆时，触发网宿安全平台的策略告警而被发现。



而另一个用户则是被网络钓鱼邮件中的附件吸引，通过未安装终端杀毒软件的BYOD设备下载了伪装成附件的恶意软件，该软件在潜伏数周后，在用户某次远程连接内网通道时，尝试向某台内网主机植入木马时被平台监测发现并拦截。网宿安全平台成功进行攻击回溯，通过对攻击样本提取分析，发现该木马为远程代码执行工具，目的是在服务器上进行提权。

2.1.2. 数据泄露事件增加44%

2022年，企业数据泄露事件已经引起了广泛的关注，但 2023 年这一问题变得更加严峻。随着企业数字化转型的加速，数据成为了企业最宝贵的资产之一，但同时也成为了攻击者的主要目标。网宿安全演武实验室观察发现，在涉及数据泄露事件的企业中，无论是大型企业还是中小企业，都难以幸免。

● 数据泄露态势

2023年网宿安全平台报告涉及数据泄露事件的企业用户，主要包括信息和互联网行业、政府、金融行业、零售业、教育行业等，泄露的数据内容包括企业代码、设计图纸、财务信息等机密数据，及用户身份信息和隐私等个人数据。

与2022年相比，网宿安全平台监测的数据泄露事件的数量显著增加44%以上，这主要归因于网络攻击手段的不断升级和多样化。黑客利用更高级的技术，如2023年日趋成熟的人工智能和机器学习，来寻找企业的系统漏洞，导致数据泄露的风险大幅上升。此外，企业远程工作的普及和常态化也为数据泄露提供了更多机会，因为员工在非传统办公环境下可能缺乏必要的安全意识和保护措施。除了外部攻击造成的数据泄露事件，内部员工窃取数据和非法销售的事件也居高不下。根据波洛蒙研究院的调查，内部员工的有意或无意行为是最常见的内部威胁形式，占网络数据泄露事件的64%。企业需要加强内部员工的安全教育和行为监控，以应对内部员工可能带来的网络安全风险。

● 数据泄露成本加剧

数据泄露的成本在2023年进一步增加。根据IBM Security的“数据泄露成本报告”，与2021-2022年相比，2023年数据泄露的全球平均成本有所上升，达到了445万美元，三年内增长了15%。据网宿安全演武实验室观察，发生数据泄露的企业，相比未发生数据泄露的企业，采取数据管控措施的付费意愿和预算投入显著增长了20%以上，这表明数据泄露的代价在不断增加，企业需要更加重视数据安全和隐私保护。

网宿安全演武实验室根据对企业用户的访谈调研发现，受到监管压力和发生潜在数据泄露的风险影响，目前80%的企业正在考虑或未来考虑实施数据安全管控措施，55%的企业正在或计划对数据防泄露技术厂商进行选型和调研。

● 数据泄露案例

以某云服务龙头企业为例，该企业的办公数据泄露呈现出以下典型场景:

其一，云平台托管着大量企业数据，这些数据同时也是公司长期运营所积累的经验及机密资产。一旦发生泄露，将会引发严重的法律风险，给公司声誉造成损害，并带来巨大的经济损失。因此，采取有效的数据保护措施对于服务提供商而言是必须达成的“硬指标”。

其二，核心岗位如财务、开发等部门的资料目前尚无安全管控措施，存在因员工安全意识薄弱而无意泄露的风险。例如，为实现备份和办公协作，员工私自将资料外发、备份、上传至云盘或云笔记等。

其三，部分员工在离职前后文件交接工作不够完整，相关文件难以获取或保留，致使公司数据资产遗失。甚至存在员工有意将数据泄露给竞争对手的情况，从而造成公司技术层面的损失。

其四，当前存在外包人员及部分员工使用个人设备进行办公的现象，外部感染病毒的设备接入内网进行横向渗透和木马植入的风险较大。此类情况已被内网主机防入侵设备识别并告警，险些导致核心数据系统被加密或遭到破坏，这引起了企业安全管理员的高度警惕与顾虑。

2.1.3. 对企业的影响

勒索软件攻击和数据泄露的威胁对企业的影响是多方面且极其严重的，这些影响不仅涉及到企业的经济层面，还会对企业的声誉、运营以及法律合规等方面造成巨大的冲击。

1.直接经济损失

勒索软件攻击和数据泄露这两类恶性事件，对于企业而言，极有可能引发极为严重且直接的经济损失。勒索软件攻击中，不法分子通过恶意手段加密企业的重要数据，并以此要挟企业支付巨额赎金，否则企业将无法恢复关键业务数据的正常使用，这不仅导致业务运营的停滞，还需要企业耗费大量资金来满足攻击者的无理要求。而数据泄露事件更是危害巨大，企业的核心机密、客户信息、财务数据等重要资料一旦被泄露，企业可能面临客户信任度下降、业务合作终止、法律诉讼赔偿等一系列问题，这些都将直接转化为巨大的经济损失，严重影响企业的财务状况和正常运营。

2.面临监管合规压力

许多关键行业都有严格的数据保护法规，一旦发生数据泄露等安全事件，企业可能会面临法律诉讼和监管机构的严厉处罚，需要承担巨额的罚款和法律赔偿责任。同时，违反相关法律法规还可能导致企业的管理层面临个人责任的追究，进一步加剧了企业所面临的危机。此外，企业需要耗费大量的时间和精力应对监管机构的严格审查，可能导致额外的整改成本。

3.企业品牌声誉受损

勒索病毒和数据窃取手段可能导致关键业务系统瘫痪、数据的丢失或损坏，这都可能导致生产停滞、供应链中断以及服务无法正常提供。这可能引发企业的信任危机，导致业务向竞争对手迁移，合作伙伴也可能重新评估合作关系。这不仅会影响现有客户的忠诚度，还会阻碍新客户的获取，对企业的市场份额和品牌形象造成长期的负面影响。

4.网络安全建设投入遭受质疑

频繁发生的勒索和数据泄露等安全事件，极有可能致使企业管理层对当前网络安全建设所取得的防护成效抱以怀疑态度。在此种情况下，信息安全团队不得不投入大量的时间和精力，用于对安全事件进行全面且深入的复盘分析，并在此基础上制定出切实有效的改进措施。申请新一期的网络安全建设预算时，若依旧遵循原有的体系和建设思路，很容易遭到管理层的质疑与挑战，被要求重新规划并给出更具有效性的新一代方案。

2.1.4 现有办公安全方案的挑战

企业办公安全面临愈加严峻的形势，然而各企业在网络安全防护建设方面又存在一些难点。网宿安全观察到企业的信息安全建设工作面临着几方面的挑战：

1.单点碎片化的防护难以抵御日新月异的攻击手法

在当今复杂多变的网络环境中，攻击手段呈现出快速迭代和不断演进的态势。然而，企业传统的安全设备往往以网络为边界，各自为战，这种单点碎片化的防御模式只能被动地响应攻击，只要存在一处短板，就可能导致整个防御体系失效。因为各个安全设备之间缺乏有效的协同机制，容易形成数据孤岛，无法形成统一的防御力量，使得攻击者能够轻易地找到防御的薄弱环节并加以突破。这使得企业在面对复杂、隐蔽的网络攻击时，无法及时发现和预警，更难以进行有效的防御和响应，从而大大增加了企业网络安全的风险。

2.信息化升级使得数据泄露途径广泛

随着业务数据化进程的显著加速，企业数据的流动不再局限于单一的场景，而是广泛分布于云端、移动端、物联网等多元化的环境之中。这种广泛的分布态势极大地增加了企业对数据进行有效管控的难度。

企业员工的办公模式日益灵活多样，他们在不同的地理位置、使用不同的设备以及依托不同的平台开展工作。这导致数据的存储和传输环节大幅增多，数据泄露的风险点不仅变得更加分散，而且难以实现全面有效的监控。与此同时，新的数字化应用和技术如雨后春笋般不断涌现，同时也不可避免地带来了未知的安全漏洞和潜在威胁，这些未知因素进一步加剧了数据保护工作所面临的挑战。

3.安全与效率难以平衡，安全运营面临重重阻力

传统的安全设备在实际应用中存在诸多问题。通常情况下，需要在终端安装多个客户端，这不仅会大量占用系统资源，还会导致安全策略难以实现统一化，从而显著增加了管理的复杂程度和难度。

在安全策略的制定和实施方面，往往面临两难困境。若采取“一刀切”的严格策略，虽然能在一定程度上增强安全性，但可能会对员工的工作效率产生负面影响，致使业务流程受到阻碍；反之，若安全策略过于宽松，则无法发挥应有的防护作用，形如虚设，无法有效保障企业的网络安全。在企业内部推行新的安全措施时，往往会遭遇较大的阻力。这主要是因为新的安全措施可能会改变员工原有的工作习惯，或者增加额外的操作步骤，从而引发员工的抵触情绪。

此外，部分关键业务所依赖的老旧系统也是企业网络安全中的一大难题。由于技术方面的限制或者出于成本的考量，这些老旧系统无法及时进行升级更新，因此容易成为安全防护的薄弱环节，为企业的网络安全带来巨大的潜在风险。

4.商业环境复杂多变，“一锤子买卖”式决策愈发谨慎

出于降低成本的考量，企业通常不愿意预先购买现阶段尚未使用到的安全能力。然而，随着业务的不断拓展以及网络威胁的持续演变和升级，为了确保网络安全防护的持续性和有效性，企业又不得不持续对安全防护措施进行升级。但此时，高昂的替换成本常常令企业陷入犹豫不决的困境。在当前市场竞争空前激烈、经济形势复杂多变的大背景下，企业所拥有的预算往往相对有限，这使得企业在做出决策时必须更加谨慎小心。任何决策上的失误，都可能导致企业在网络安全方面遭受重大损失，或者因过度投入而影响整体的经济效益和竞争力。

在复杂的商业环境中，企业在网络安全领域面临着成本与效益之间的艰难权衡，“一锤子买卖”式的决策方式已不再适用，需要更加精细和灵活的策略来平衡安全与经济利益。

2.2. 企业办公安全建设指南

2.2.1. 办公安全设计原则

2.2.1.1. 以身份为中心，落地零信任理念

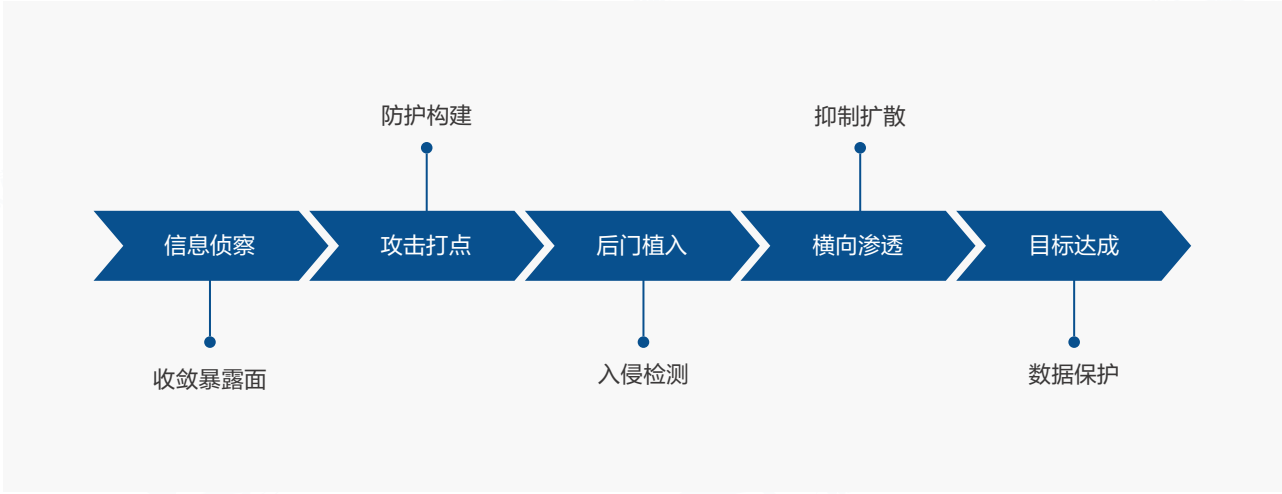
数字化转型下，以内外网作为“信任”边界的传统网络安全架构难以应对边界的泛化，而新一代的办公网络安全防护理念，它的关键在于打破默认的“信任”，也就是“零信任”的思想。通俗来说，就是“持续验证，永不信任”。默认情况下，企业内外部的任何人、事、物均不可信，应在授权前对任何试图接入网络和访问网络资源的人、事、物进行验证。

零信任体系的落地，需要先构建一个以身份为中心的策略模型以实现动态的访问控制。以身份为中心，可以根据用户的角色、职责、访问历史等多维度的信息来精细地授予访问权限，实现更精准的访问控制，降低过度授权或授权不足带来的风险。其次，还能够实现动态的权限管理。随着用户的工作需求、职位变动或者风险状况的变化，其访问权限可以及时调整。这种动态性能够更好地适应业务的快速变化和安全需求的更新。再者，以身份为中心能够集中管理和监控用户的访问行为，便于发现异常和潜在的安全威胁，快速采取相应的措施进行应对和处置。

2.2.1.2. 构建端到端的风险管理体系

在办公安全的设计过程中，采纳风险管理的原则具有极其关键的重要性。这一原则要求企业不能仅仅局限于在网络的边缘位置进行防御，而是需要针对整个网络环境里的每一个潜在风险点，开展全方位、无死角的风险管理工作。

为了实现这一目标，企业必须在从用户端至服务端的整个办公访问流程当中，对所牵涉到的各类风险进行精确的识别、全面的评估、有效的缓解以及持续的监控，进而构建起一个全面且体系化的“端到端”的风险管理体系。具体而言，应当在设备层、网络层、应用层、数据层等各个不同的层次之上，部署设置具有灵活性的安全防御举措。即使攻击者成功突破了某一层级的防线，后续仍然存在多层防线能够对攻击进行阻止或者减缓其进一步发展的势头。同时，企业还有必要构建一个能够主动适应不断变化威胁环境的安全防御体系。这个体系要具备高度的灵活性和适应性，能够根据威胁的变化及时调整防御策略，确保企业业务能够在安全的环境中持续发展，不受网络安全威胁的干扰和影响。



这就要求企业的网络安全防护方案中，设备层、网络层、应用层、数据层等各层的安全防护机制要能够实时共享风险信息和攻击数据。当某一层检测到异常或攻击时，能够迅速触发其他层的相应防护措施，协同工作进行处置，形成一个紧密配合、高效运作的整体防御网络，最大程度地保障企业办公网络的安全和业务的连续性。

2.2.1.3. 采用一体化方案，兼顾效率与安全

现代企业面临的安全威胁复杂多样，涵盖网络攻击、数据泄露、内部人员违规等。企业办公安全建设应采用一体化的防护体系，整合多种安全技术和策略，从网络边界到终端设备，从应用程序到数据存储，对各种办公场景进行全方位的保护。

一体化的安全防护方案，可以帮助企业提高效率和降低成本。在多样复杂的办公场景下，如果分别采用独立的解决方案，会导致管理复杂、维护成本高昂。一体化方案能够整合资源，减少重复投资，通过集中管理和统一策略配置，提高管理效率和降低运营成本。此外，一体化防护方案可以确保一致性和连贯性，避免各个独立的方案可能存在策略不一致、技术不兼容等问题，导致安全防护出现漏洞。

在数据安全保护方面，对于不同密级的数据，企业往往需要采取不同程度的保护措施。企业可以在确保敏感数据安全的同时，不过度限制一般性数据的正常流通和使用，从而在数据安全和办公效率之间找到平衡。因此需要采取一体化数据防泄漏方案，从而满足企业开展全面、高效且灵活的数据安全保护手段，兼顾了办公效率和数据安全，避免了因采用多种分散的安全措施而导致的管理混乱和效率低下。

一体化的防护方案还有助于降低管理成本，统一的体系便于集中管理和监控，减少了重复投入和资源浪费，提高了资源的利用效率。

2.2.1.4. 可灵活部署，支持升级演进

企业办公安全方案的设计应当充分考虑到其能够随着企业的发展实现灵活的升级与调整。

在企业的发展进程中，其规模处于不断变化的状态。初创时期可能是小团队，而后可能迅速扩张，员工数量大幅增加，业务范围持续拓展。这种情况下，必然需要相应提升安全防护的覆盖范畴和能力，从而适配新的办公网络架构以及更多的访问需求。同时，业务类型和模式的转变会催生新的安全风险。例如，当企业从传统业务转向数字化服务时，数据量会剧增，交互方式也会发生重大改变，原有的安全防护方案必须及时进行升级与调整。

技术的快速更新迭代对安全方案提出了跟进的要求。云计算、物联网、移动办公等新的技术应用不断涌现，如果企业不能及时对安全部署做出调整，就极有可能出现防护的空白区域。此外，伴随企业的发展，其在市场中的地位以及所面临的竞争环境也会发生变化。这可能会引发竞争对手更多的关注，甚至遭受恶意攻击，因此需要增强安全防护的强度并提高其针对性。

为确保企业能够持续稳定地发展，办公安全方案的设计理应能够实现无感升级调整，并且能够依据企业的发展变化灵活地部署和实施防护策略。

2.2.2. SASE一体化办公安全方案

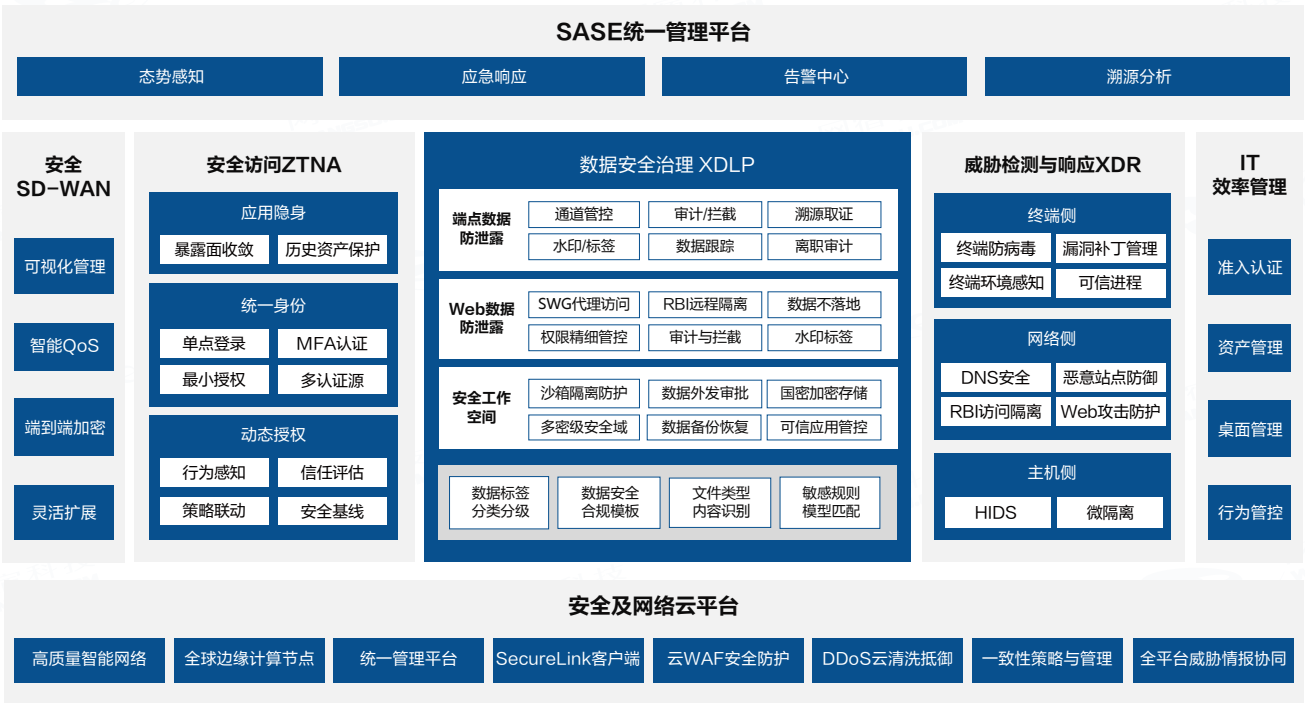
SASE架构提供了一个符合当今数字化企业需求的网络安全解决方案。它的灵活性、简化管理、成本效益，让它成为一种符合未来趋势的办公安全建设方式。随着企业对安全和网络效率要求的不断提高，采用SASE架构的企业将更具竞争优势和适应力。

1）降低企业和组织的网络安全风险：SASE通过基于身份的访问控制，以及集成的安全策略和服务，能够更有效地防御安全威胁，减少数据泄露和攻击的风险。统一的监控和分析也有助于快速识别和主动响应潜在的安全事件。

2）提高企业和组织的网络效率和业务灵活性：云原生的SASE平台通过提供就近接入的服务节点和高效的网络连接服务，优化了网络性能，实现全球范围的资源共享和协同办公，促进企业间的合作和创新。这种灵活性使得企业能够快速适应远程办公的扩展和业务需求的变动，从而保持业务连续性和竞争力。

3）降低企业和组织的IT成本：传统的网络安全解决方案需要大量设备和维护成本，SASE通过边缘+云安全，减少软硬件投入和维护费用，从而降低企业的资本支出和运营成本。企业可以根据实际使用情况来按需按模块灵活购买SASE服务。

针对当前办公网络安全威胁态势，网宿安全基于Gartner SASE安全框架，设计开发了一套一体化办公安全方案。网宿SASE一体化办公安全方案融合安全SD-WAN、零信任访问ZTNA、数据安全治理XDLP、威胁检测与响应XDR、IT效率管理和统一态势管理进行全流量的防护，产品模块All In One，轻量化地为企业带来更安全、更高效、更便捷的办公服务。



2.2.3. SASE方案实施建议

企业的发展是分阶段的，不同阶段对安全的重点需求可能不同。SASE方案的实施建设分步可以根据企业当前的业务重点和紧迫需求，优先实施关键部分，使安全建设与业务发展更紧密地结合。同时，分布开启安全策略也能降低风险和复杂性。

建议企业可以按照以下三个阶段，选择合适的建设目标：

2.2.3.1. 基础办公，快速落地零信任，轻量数据保护

建设重点：

企业发展初期，聚焦办公访问安全，从暴露面收敛切入，通过总分组网、远程办公、无感审计，实现基础办公环境和底层云安全网络架构的搭建，打造局部用户的安全接入能力，夯实安全能力底座建设。

1、快速收敛暴露面：企业面向互联网暴露的IT资产是第一道风险，也是企业在实施SASE方案最优先、见效最迅速的手段。通过实施零信任，帮助企业快速实现互联网IT资产的“网络隐身”，让外部信息侦察和扫描无从发起。
2、身份管理及访问控制授权：以身份为中心的最小授权原则，灵活而严格管理应用的访问权限，并实施轻量数据外发审计，对用户无感知，推广阻力小。
3、用户访问体验提升：传统的办公网络方案无法有效保证跨网、全球办公场景下的网络访问质量，依托全球SD-WAN安全加速网络，可以给用户带来极致的访问质量和办公体验。

推荐场景：

1）企业员工出差/远程办公、BYOD安全办公接入和轻量数据保护
2）第三方合作伙伴、上下游供应商、外包等远程接入，精细化管理身份和访问权限
3）护网、等保合规下的内网安全加固，收敛互联网暴露面，解决VPN 0day隐患

2.2.3.2. 高效办公，全面零信任，全面数据保护

建设重点：

企业快速发展阶段，进一步优化员工办公体验，由浅入深地实施多维度安全策略，立体化提升办公防护水位，并实现数据防泄露全场景覆盖。

1、全面零信任实施：从局部的远程办公接入，推广到全企业无论内外网都实施零信任。实现内外网的统一集中可视化运营，一站式管理企业的软硬件资产，安全更全面，建设企业安全合规的规范化体系。
2、立体化风险防护：融合XDLP、XDR、网络准入和ZTNA联动，通过UEBA深度分析，持续动态授权，将风险横向移动降至最低，提高风险处置的及时性和准确度，提升整体安全水位，提高运营效率。
3、数据防泄露全场景覆盖：针对不同用户、不同终端、不同数据和不同应用的数据防泄露全场景全通道无死角覆盖，建设覆盖数据全生命周期的分类分级管控体系。

推荐场景：

1）全球员工、第三方安全办公协同，提升效率
2）上下游供应商、代理商、外包等第三方远程接入安全，动态信任评估
3）针对BYOD到移动办公，从第三方合作到外包研发，从低敏到高敏业务应用，实施多级数据管控策略

2.2.3.3. 主动全局防护，持续安全运营

建设重点：

企业发展到成熟稳定运营的阶段，建设主动防御体系，应对复杂攻击，结合IT管理工具提升办公安全运营效率。

1、主动风险识别：通过SASE方案接管访问内网的所有流量，丰富的深度威胁检测和增强威胁防御能力，全网终端威胁可视化，风险识别主动化，威胁处置自动化，审计溯源可视化，全面提升终端安全水位，打造企业安全管理体系化。
2、第三方安全联动：可以设置与企业传统安全的日志对接，实现威胁的协同与联动处置，最大化实现现有安全设备投资的价值体现。
3、IT高效运营：将终端、网络与安全集成一体化管理，订阅式服务，按需购买，成本更可控；性能消耗小，用户感受好，提升终端运维和安全管理效率。

推荐场景：

1）钓鱼、勒索防护
2）攻防演练、一机两用
3）高效一体化运营

第三章 思考讨论：降本增效背景下的体系化主动安全能力建设

3.1. 企业安全建设现状观察

3.1.1. 网络安全立法与企业合规现状

自2017年《网络安全法》实施以来，中国的网络安全立法进程显著加快，2020年，《个人信息保护法》与《数据安全法》的出台，进一步细化了个人信息保护与数据安全管理的法律框架，标志着中国网络安全治理进入了精细化、全面化的新阶段。此间，诸如《关键信息基础设施安全保护条例》等配套法规的制定，强化了对关键领域安全的特别监管，也逐渐形成了全面而深入的网络法治体系，截止到2024年6月，中国已制定出台了150多部网络领域法律法规，标志着网络法治体系的“四梁八柱”已初步搭建完成。

纵观2023年，受新冠疫情影响，全球面临经济增速下降甚至陷入衰退，在此过程中，网络安全的本质以及立法进程也发生了诸多变化，本章结合专业的行业观察总结了2023年网络安全合规的“变”与“不变”：

3.1.1.1. 网络安全合规之“变”：安全内涵的深化与技术驱动的挑战

- **安全内涵的深刻变革**

  2023年，安全的内涵从“绝对安全”向“相对安全”转变，强调安全是达成目标的手段，而非终点。这一转变反映出，在网络领域，绝对安全难以实现，而确保在动态环境中维持安全状态成为了新的目标。数据安全不再孤立存在，而是与产业发展紧密结合，形成了“不发展是最大的不安全”的共识。

- **跨境数据流动的新挑战**

  跨境数据流动成为网络安全领域的新焦点，中国构建了“3+3”跨境数据流动制度框架，试图在数据保护与数据利用之间寻找平衡。《个人信息出境标准合同办法》和《数据出境安全评估办法》的实施，标志着中国在数据跨境流动监管上迈出了实质性的步伐。特别是对自由贸易试验区的创新举措，体现了对跨境数据流动管理的灵活性和前瞻性的探索。

- **AI与大模型技术驱动行业变革**

  新兴技术，尤其是人工智能（AI）和大数据，为网络安全市场带来了“变”的推动力。以ChatGPT为代表的生成式AI技术的快速发展，不仅推动了创新服务，也带来了数据安全、个人信息保护等新挑战。《生成式人工智能服务管理暂行办法》等法规的出台，标志着中国开始系统性地应对新技术带来的安全问题，强调在促进创新的同时，加强安全与合规监管，确保技术的健康发展。

3.1.1.2. 网络安全合规之“不变”：合规导向与双轮驱动的市场底色

“合规”导向依旧坚挺

在2023年，中国网络安全市场的一个显著“不变”特征是其依然以合规为导向。尽管全球范围内不稳定因素频现，但中国网络安全立法体系的成熟构建为市场提供了稳定的法律基础。《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规的相继出台，确立了以法律为基石的网络空间秩序，形成了以数据安全和网络安全为双引擎的市场驱动力。企业对于满足网络安全等级保护、数据合规等要求的投入持续加大，确保了在数字经济时代下的稳健发展。

数据安全与网络安全双轮驱动

数据安全与网络安全如同并驾齐驱的两轮战车，共同推动市场向前。数据作为数字经济的核心要素，其安全直接关联到国家安全、公共利益及产业利益。在“以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展”的理念指导下，数据安全与网络安全相辅相成，共同构成了市场稳定增长的坚固基石。

3.1.2. 成本导向的合规痛点

仅以合规驱动的安全性可能会导致组织脱离或忽视真正的业务安全风险和保护需求，“成本导向”的合规观点存在诸多问题，具体来说:

安全投入存在浪费的风险

随着《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规的实施，以及《数据出境安全评估办法》、《个人信息出境标准合同办法》等一系列配套规定的出台，企业需要投入大量的资源来理解和遵循复杂的合规要求。

与此同时，企业在衡量合规成本与监管风险，以及应对频繁更新的法规时，盲目的以合规导向做安全建设，有可能导致安全投入的浪费。

合规重复投入导致的效率低下

网络安全法规与国家标准、行业标准之间存在交叉重叠现象，导致企业在被动执行合规评估与整改工作时，往往会出现重复投入。比如，等级测评、密码应用安全评估、数据安全评估、风险评估和个人信息保护等工作，有近40%的任务存在重叠，这不仅消耗了大量的人力、物力和财力，还降低了合规效率。企业需要在基于全局视角，体系化的评估安全投入，避免不必要的重复工作。

安全投入与实战能力的不对等

在数字化加速发展以及攻防对抗逐渐提升的背景下，企业虽加大了安全投入，但实战能力提升并未同步跟进，形成明显的不对等现象。尽管采用了先进的防护技术和设备，构建了纵深防御体系，但在“云、大、物、移”的复杂环境下，以及近年来人工智能技术的发展，网络安全防护技术的演进速度落后于威胁演变，导致防护盲区。加之互联网暴露面的持续扩大，安全技术间的协同不足，以及在应对安全事件时的协同机制不健全，进一步加剧了这一矛盾。尤其在专业人才方面，缺乏既精通技术又懂实战的复合型人才，难以高效应对日益复杂的网络安全挑战。这种投入与实战能力的不对等，成为制约企业安全防护效能的关键瓶颈。

3.1.3. 从合规驱动到业务驱动：安全战略转型的必然之路

在全球经济动荡和新冠疫情等多重因素影响下，企业面临前所未有的经济压力，纷纷采取降本增效策略。国际货币基金组织（IMF）2023年世界经济展望报告显示，全球经济增长放缓，企业利润空间压缩，促使企业对每一笔开支的效益比有了更高要求。网络安全预算同样受到严格审视，企业在确保合规的同时，寻求成本效益最大化，成为当务之急。

转变观念，从被动合规到主动安全

过去，许多企业对网络安全投入的态度往往是被动应对，以满足监管政策作为最低要求。随着网络安全法规的密集出台，企业合规成本上升，但却并未换来实战能力的同步提升。因此，企业需转变观念，从被动合规转向主动建设体系化安全。这意味着安全策略不仅要符合法规，还要与业务发展紧密结合，通过风险管理导向的安全体系，优化成本，提升竞争力。

积极采用“云安全”技术：成本优势与业务敏捷性的结合

云安全技术的发展为这一转变提供了技术支撑。云服务提供商通过规模效应和技术创新，提供成本优势与业务敏捷性兼顾的安全方案。相比传统的本地部署，SaaS化的云安全服务，能够利用大数据分析、人工智能等技术，提供高效威胁检测与响应，减少攻击窗口期；云安全服务的订阅模式允许企业按需付费，减轻财务压力；云服务提供商负责维护和升级，可减少维护成本；云安全解决方案的集成性和可扩展性，能够帮助企业灵活调整安全服务级别，实现资源最优配置。

建立主动安全运营体系：企业安全能力的进阶

数字时代，企业面临安全合规、多云管理、高级威胁、应急响应等多重挑战。企业数字化转型早期阶段采用的本地烟囱式安全架构，已不适应当前需求，企业需建立主动安全运营能力，通过持续监控、分析、响应和优化，实现安全防御的主动性和前瞻性。

然而，自行组建24小时运作的安全团队，并维持一个先进的安全运营中心，对多数企业而言并非易事。基于云的网络安全服务（简称SECaaS）就成为了破解难题的关键。云端运营模式突破传统边界安全限制，通过建立统一的网络安全运营平台，能够提供集成安全功能和基于大数据与AI的SaaS化安全运营服务，结合本地化硬件产品，以云地协同方式，提供全天候、持续、专业的安全运营服务。

3.2. 体系化主动安全能力建设思考

通过前面的分析不难看出，在当前复杂多变的网络安全环境以及企业降本增效的背景下，企业必须从被动防御转为主动出击，构建以云安全为核心、云地协同的主动安全运营体系。这不仅是为了能在成本可控的前提下构建更加高效的安全防护体系，以应对日益严峻的安全威胁，更是企业数字化转型成功的关键。通过遵循网络安全能力成熟度模型，持续优化安全体系，实现安全与业务的深度融合，企业才能在保障数据安全的同时，推动业务的稳健发展，赢得数字时代的竞争优势。接下来，网宿安全将围绕“基于网络安全能力成熟度的安全体系完善”以及“基于云端+本地协同的主动安全运营体系”两个章节来为企业提供体系化主动安全建设的指导。

3.2.1. 基于网络安全能力成熟度的“实战化”安全体系完善

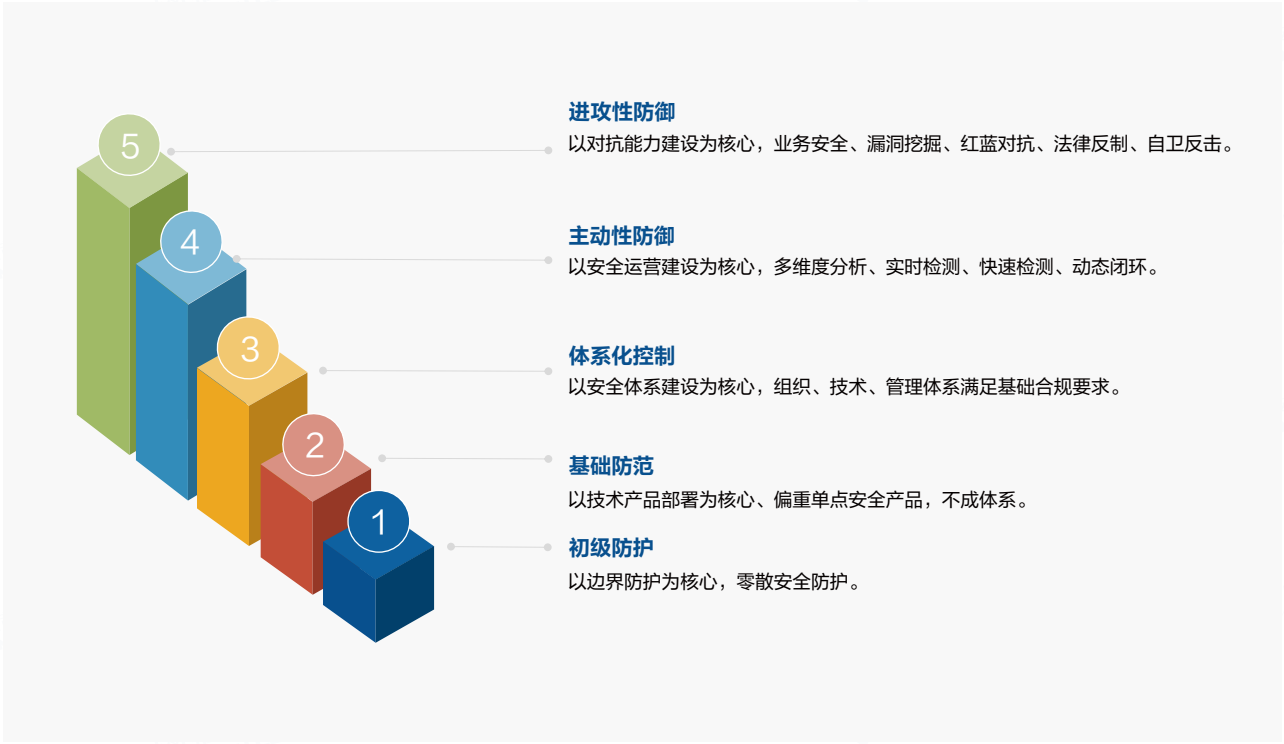
3.2.1.1. “实战化”网络安全体系建设方法论

在数字化转型的浪潮中，网络攻击日益呈现“实战化”特征，其隐蔽性、实时性、即时响应及人机协同特性对企业的安全防护提出了更高要求。实战化体系建设，强调在真实攻防环境下快速发现、定位、处置及恢复的能力，是企业应对复杂安全挑战的关键，网宿安全认为，构建“实战化”网络安全体系需要从安全能力评估、安全体系完善以及实战能力验证等3个阶段进行逐步完善。

1. 安全能力评估：基于网络安全成熟度的能力评估

安全成熟度调研

首先，基于网络安全能力成熟度模型进行自我评估，从政策、流程、技术、人员等多维度诊断企业当前的安全状况。识别安全短板，明确改进方向，根据企业安全建设所处的接触以及进阶的目标，制定评估符合企业要求的“能力成熟度模型”。



端到端风险评估

进行全面的安全风险评估，包括资产识别、威胁建模、脆弱性扫描，特别是对关键业务系统、数据资产进行重点审查，量化风险等级，并输出能力指标差距分析报告，为后续安全体系的完善提供数据支持。

安全体系建设

根据能力指标差距分析报告，编制建设方案。

2. 安全体系完善：围绕核心维度加固防线

端点安全强化

部署先进的端点防护解决方案（EPP/EDR），结合行为分析与机器学习技术，实现对终端设备的实时监控与威胁防御，提升对恶意软件、钓鱼攻击等的防范能力。

网络与云安全加固

构建多层次的网络防御体系，包括下一代防火墙、入侵检测与预防系统（IDPS）、Web安全网关（SWG）以及主机安全（HIDS）等，确保云环境与本地网络的安全互联与数据保护。

应用安全与数据保护

实施应用安全测试（SAST/DAST），加强代码审查，防止应用层漏洞。采用数据加密、访问控制、数据丢失防护（DLP）等技术，确保敏感数据在传输和静止状态下的安全。

统一安全管理

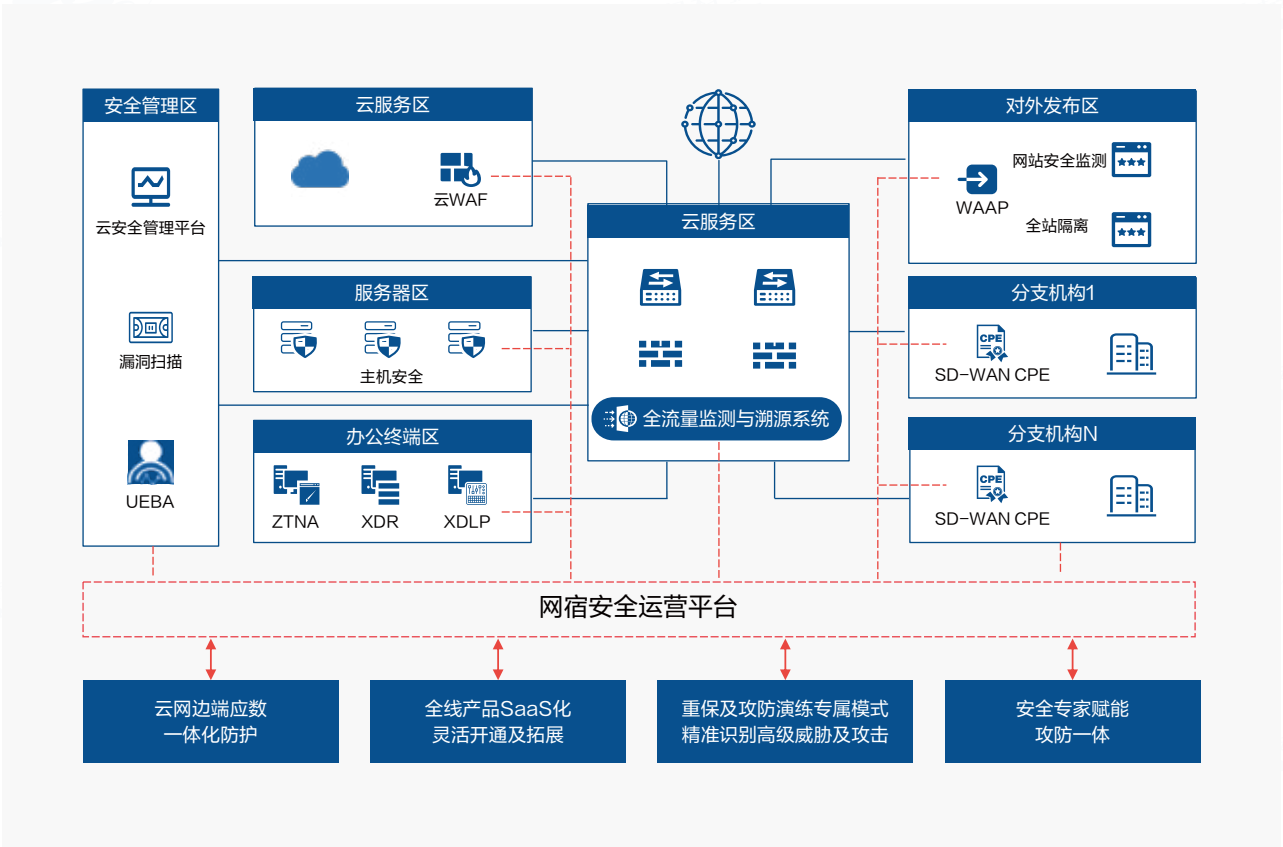
建立统一的安全管理平台，整合安全日志、事件管理（SIEM）、安全编排自动化与响应（SOAR）等功能，实现跨系统、跨环境的安全策略统一与高效响应。

3.2.1.2. “实战化”网络安全体系建设最佳实践

在安全建设的实际落地方面，网宿建议企业应当通过践行体系化主动安全驱动的常态化安全理念，建设从云、网络、端点、应用到数据的全链路防护，同时覆盖日常安全管理过程的发现、检测、防护、响应、运营的全流程防护，建立起云端SaaS化的敏捷安全运营体系，同时，以开放平台的模式与本地实现云地协同，才能实现安全防护的效果最大化。

网宿安全凭借多年的云安全技术积累，并结合为众多行业用户提供体系化建设的实践经验，总结出了集云、网络、端点、应用以及数据为一体的体系化主动安全防护架构，具体来说：

- 在部署云安全管理平台，漏洞扫描以及UEBA，对全网威胁情况提前感知，实时研判；
- 在对外发布区，部署WAAP全站防护对业务及应用进行全方位防护，并通过全站隔离技术提高关键系统的防护等级，结合网站安全监测，对Web应用风险进行实时感知；
- 在云服务区，部署云WAF，对Web应用进行精准防护，协同威胁情报实时响应，秒级封禁；
- 在服务器区，部署主机安全探针，守好纵深防御的最后一道防线；
- 在办公终端区，部署ZTNA、EDR以及XDLP，对远程访问、终端威胁感知以及数据防泄漏进行全生命周期管理及防护；
- 在核心交换区，部署全流量监测与溯源系统，对入侵行为进行检测并留存证据；
- 最后，在分支机构，通过部署SD-WAN组网与总部进行安全连接，避免旁路攻击以及供应链攻击。



基于此，网宿安全可以帮助企业构建一个先进的网络安全架构，产品能力覆盖了企业各个分区的防护，整个平台不仅能够做到云网边端应数的一体化防护，同时也支持SaaS化，满足企业需要快速开通及拓展的需求，通过云端的安全运营平台，帮助企业做好持续的检测与响应。

3.2.2. 基于云端+本地协同的主动安全运营体系

3.2.2.1. 主动安全运营体系思考

1. 企业安全管理挑战分析

在数字化转型的背景下，企业面临着前所未有的安全威胁与挑战。传统的静态防御模式已难以适应攻击手法的多样化与复杂化，被动响应往往导致防御滞后于攻击，安全形势愈发严峻。

被动防御的局限性	攻防不对等的现实	资源与预算的限制
传统的安全体系侧重于构建边界防御，如防火墙、入侵检测系统等，但这种静态防御模式在面对高级持续性威胁（APT）、零日攻击时显得力不从心。攻击者利用未知漏洞或社会工程学技巧，能够轻易绕过传统防御，对核心资产造成损害。	攻击者只需找到一个突破口，而防守方却要确保所有环节无懈可击。这种攻防不对称性使得防御成本远高于攻击成本，企业往往在资源有限的情况下，难以全面覆盖所有潜在威胁。	安全投入与企业利润之间存在矛盾，很多企业在面对安全预算时往往采取保守态度。此外，安全专业人才的短缺也制约了安全运营的效率与质量，企业难以组建一支高素质的安全团队，进行全天候的安全监控与响应。

2. 云端安全运营的优势分析

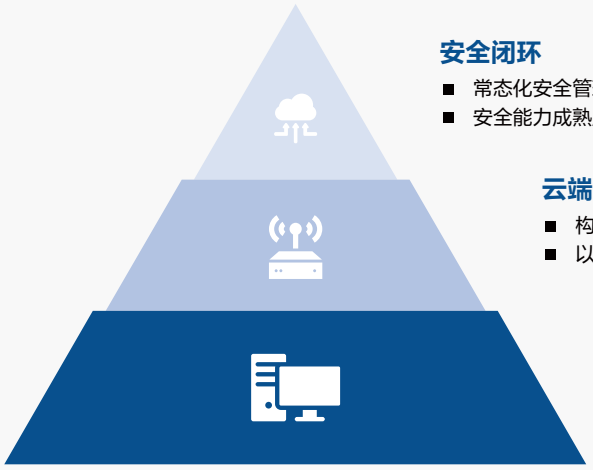
云安全运营作为一种新型的安全管理模式，以其独特的技术优势与运营模式，为企业提供了一种更为高效、灵活的安全解决方案。

资源弹性与成本优化	集成化与自动化响应	实时情报与智能分析
云安全服务基于订阅模式，企业无需大规模前期投资，可以根据实际需求动态调整资源，实现成本的精细化控制。同时，云平台的集中管理与自动化工具显著降低了运维成本，提高了安全运营的经济性。	云安全运营平台集成了多种安全功能，如威胁检测、事件响应、安全编排自动化与响应（SOAR）等，实现了安全事件的快速识别与自动化处置。这种集成化与自动化响应能力大大提升了安全运营的效率与精准度。	云安全服务能够接入全球威胁情报，结合大数据分析与机器学习技术，实现对威胁的实时监测与智能预警。企业可以基于云平台的分析结果，制定更具针对性的安全策略，提前防范潜在风险。

3. 主动安全运营建设理念

因此，构建主动安全运营体系是企业实现安全防护升级的必由之路，企业在完善安全运营体系时，应该首先以“风险管理”作为核心理念，将全域风险意识，包含攻击者风险、资产风险、业务风险以及组织风险等，贯穿在整个安全运营体系建设的全过程：

全域风险管理	云地协同的运营模式	常态化的安全能力验证
主动安全运营强调从全局视角出发，覆盖所有业务流程、技术架构与人员行为，实现风险的全面识别与管理。企业应定期进行风险评估，制定应急预案，确保在任何情况下都能迅速响应，将损失降至最低。	结合云安全运营的优势与本地安全的必要性，构建云地协同的安全运营模式。云端负责提供实时情报、集中管理与自动化响应，而本地则侧重于物理安全、数据加密与内部网络的深度防护。通过两者的紧密配合，实现安全资源的最优配置与协同作战。	安全能力的持续验证是主动安全运营体系的重要组成部分。企业应定期开展攻防演练、渗透测试等活动，检验安全体系的有效性，提升安全团队的实战能力。同时，通过常态化的安全培训与意识提升，确保每一位员工都能成为安全防线的一部分。



安全闭环
- 常态化安全管理（安全意识、钓鱼演练等）
- 安全能力成熟度评估（红队模拟、BAS等）

云端安全运营
- 构建云端SaaS化的敏捷安全运营体系
- 以云地联动为核心的安全生态

风险管理
- 从合规驱动、业务驱动到“风险驱动”
- 全域风险意识：攻击者风险+资产风险+业务风险+组织风险

3.2.2.2. 主动安全运营体系建设实践

1. 主动安全运营体系建设思路

构建主动安全运营体系，旨在实现企业安全防护从被动响应向主动防御的战略转变。这一转变不仅要求技术层面的革新，更涉及安全策略的深度调整与优化。建设思路的核心在于，基于现状的全面梳理与评估，科学判断哪些云端与本地安全运营的重点，以及如何设计云地协同的安全运营模式，以期实现资源的最优配置与安全效能的最大化。

现状梳理与评估的考量维度：

- **技术可行性：**评估现有安全功能的技术栈是否与云平台兼容，能否顺利迁移并维持原有效能。
- **数据敏感性：**根据数据分类与行业监管合规要求，判断哪些数据适合云端安全运营，哪些因涉及隐私、法规等因素需保留在本地。
- **业务影响度：**考量安全功能的中断或迁移对核心业务的影响，优先保证业务连续性。
- **成本效益比：**分析迁移成本、运维成本以及云服务带来的经济效益，确保投入产出比合理。

云端及本地安全运营规划：

1)云端安全运营重点建议：

威胁情报分析与共享	云端的全球威胁情报数据库与大数据分析能力，能提供更全面、实时的威胁情报
分布式第一道安全防线	基于边缘分布式的云安全防线，如云WAF、DDoS、API安全等应用安全防护能力
安全日志管理与分析	云安全管理平台的弹性存储与处理能力，适合大规模日志的集中管理与分析
自动化响应与编排	云端的自动化工具与智能响应机制，能够快速处置安全事件，减少人工干预
云原生安全服务	如零信任安全访问（ZTNA）、安全组网SD-WAN、应用安全网关（SWG）、主机安全（HIDS）等，专为云端运营设计，实现云端资源的深度防护

2)本地安全运营重点建议：

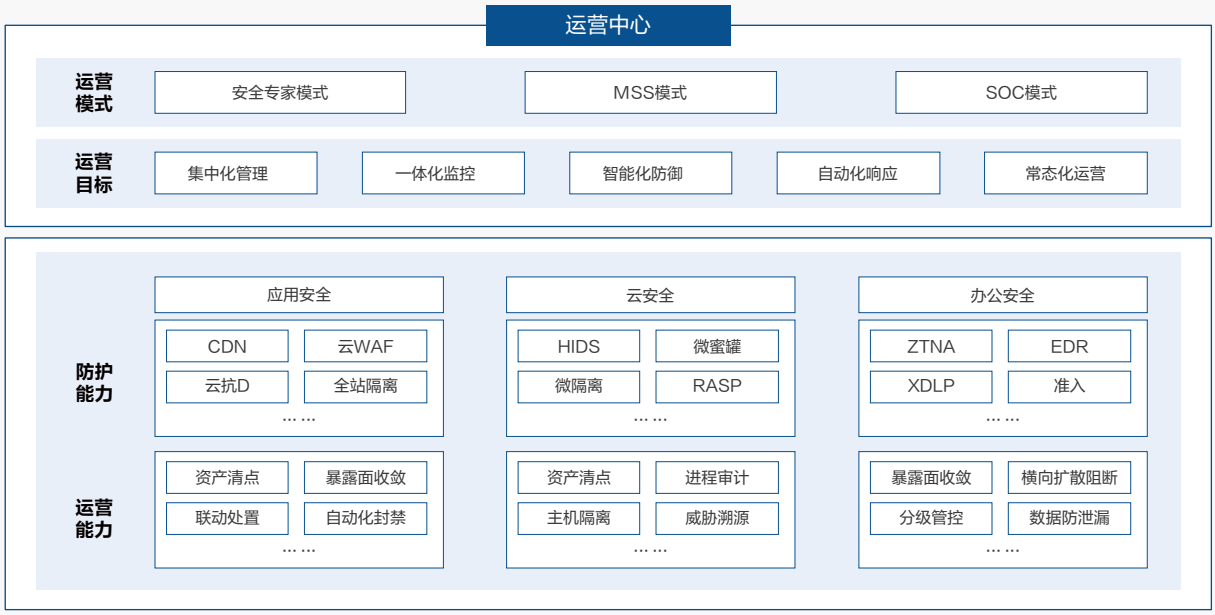
物理安全与环境控制	如数据中心的物理访问控制、温湿度监控等，需本地部署以确保物理环境安全
高敏感数据加密与存储	涉及核心商业秘密、客户隐私等高敏感数据的加密与存储，宜保留在本地，通过终端安全（EDR/EPP），以及数据防泄漏（XDLP）等能力遵循合规要求
内部网络深度防护	如内部网络的防火墙、入侵检测系统（IDS）等，用于防范内部网络的横向渗透
关键业务高可用性保障	对于高可用性要求极高的业务系统，通过本地冗余以及灾备的方式进行可用性的保障

2. 主动安全运营体系建设实践

网宿云端安全运营体系实践

网宿安全基于应用安全、云安全以及办公安全等核心能力，通过分布式SaaS化安全能力，将应用、云和办公安全做集中化的安全管理以及一体化的监控，平台可以做到持续的智能化防护和自动化响应，协助企业做好常态化运营工作。

运营模式上主要分为安全专家模式、MSS模式以及SOC模式：



云地协同的安全体系架构

网宿的云端运营平台能够汇聚来自多源的安全数据，实现统一的监控、分析与响应。自动化响应机制基于预定义策略，对安全事件进行即时处置，显著提升了响应速度与处置效率。

运营平台可以利用大数据分析与机器学习技术，对海量安全数据进行深度挖掘，识别潜在威胁模式，提前预警未知风险。全球威胁情报的实时接入，确保企业能够及时调整安全策略，抵御最新攻击手法。

作为安全运营的中枢，能够整合企业云上云下的安全资源，实现跨部门、跨地域的协同作战。标准化的事件响应流程与集成的安全编排工具，确保了威胁发生时，各部门能够迅速联动，形成合力，有效控制风险扩散。

第四章 总结与展望

体系化主动安全能力构建是企业安全建设进入深水区的必经阶段。本篇报告先重点从Web安全和办公安全这两个企业安全建设的核心保障场景出发，进行了详细的威胁态势分析，总结2023年核心态势观察如下：

- Web应用程序攻击持续快速增长，Web业务面临从网络层、应用层到数据层、业务层多维度风险升级的攻击威胁，核心威胁类型包括漏洞利用攻击、DDoS 攻击、恶意爬虫、营销欺诈、API滥刷等攻击类型，生成式AI的发展则让网络攻击更加的隐蔽与自动化、智能化。
- 勒索攻击与数据泄露已成为当今企业最为关注的两大核心安全威胁，这两类安全事件数量快速上升，正严重阻碍企业正常运营发展的脚步，数据泄露的成本也进一步加剧。其中，在勒索攻击事件中统计发现漏洞利用、钓鱼邮件、弱口令做为勒索攻击中的前三类主要攻击手段；而在数据安全方面，内部威胁引发的数据泄露事件数量则已超过了外部攻击。
- 网络安全威胁更加复杂以及充满未知，网络服务模式和办公模式的不断升级转变让威胁和风险更加的泛化，传统的防御思路存在安全产品碎片化、运营效率低下、难以应对新兴威胁、成本偏高等诸多困境，企业需要更具现代性的Web安全、办公安全防御体系。

结合上述网宿安全观察到的2023年核心威胁态势，报告重点介绍了当前业界新一代的一体化安全防御架构——WAAP和SASE，并阐述了企业如何用其全面保障Web安全和远程办公安全这两个核心场景、落地“体系化主动安全”建设。

报告最后部分，我们则上升到更高的企业整体安全建设维度，结合当前降本增效背景，对“体系化主动安全”内涵进行了思考，提出企业安全建设理念需要从政策被动导向的“合规驱动“转向真正价值导向的“业务驱动”，积极拥抱云安全技术，借助云安全服务的成本效益、可扩展性、安全能力高度整合、专业服务支持等优势，通过基于“网络安全能力成熟度”的方法论，去构建云端+本地协同的安全防御和安全运营双体系，实现真正可用于实战的主动安全防御体系。

附录

报告编写：网宿安全演武实验室

网宿安全演武实验室设立于网宿厦门研发中心，“演武”源于民族英雄郑成功为收复台湾而在厦门操练水兵的演武场。如今，网络作为第五空间，网络安全已经成为新的战场。网宿安全希望继承先贤遗志，建设能攻善防的安全体系，为守护国家网络空间的完整和安全贡献一份力量。

演武实验室拥有超过30位攻防研究专家，专注于应用安全、数据安全领域，重点研究SASE和WAAP安全架构、零信任安全体系，具备系统化的渗透、逆向等Web攻防技术工具体系，拥有行业领先的Web安全威胁情报系统。

演武实验室的诸多研究成果已应用于网宿全站防护（WAAP）、SASE一体化办公安全方案等产品服务，并作为CNCERT(国家互联网应急中心)网络安全应急服务支撑单位（乙级）、国家信息安全漏洞库（CNNVD）技术支撑单位（二级），在国家级安全领域也发挥了重要作用。

演武实验室积极分享关于Web安全和办公安全的研究成果，不仅承担了网宿安全《互联网安全报告》、《零信任安全白皮书》，《SASE安全访问服务边缘白皮书》等研究报告的编写任务，为行业提供详尽的安全态势分析和趋势预测，同时也活跃于freebuf等安全社区，推动安全技术的广泛交流与应用，持续赋能国家、行业和区域的攻防两端。

版权信息