安恒信息
DAS-security 安全中国

全球网络安全创新 500 强｜专业网络信息安全产品和服务解决方案提供商

CNCERT/CC网络安全应急服务支撑单位证书（国家级）
国家信息安全测评信息安全服务资质证书（安全工程类三级）
国家信息安全测评信息安全服务资质证书（风险评估二级）
国家信息安全测评信息安全服务资质证书（安全开发类一级）
信息安全服务资质认证证书（风险评估一级）
信息安全服务资质认证证书（应急处理一级）
中国国家信息安全漏洞库（CNNVD一级技术支撑单位）
北京奥运会、国庆60周年庆典、抗战胜利七十周年、历届世界互联网大会、G20峰会、金砖峰会、
一带一路高峰论坛、十九大、上合组织青岛峰会等重大活动网络安全保障提供商

东北及华北地区	北京	哈尔滨
	天津	郑州
	济南	太原
	沈阳	呼和浩特
	长春	石家庄
华南及西南地区	广州	成都
	贵阳	重庆
	海口	福州
	南宁	昆明
	深圳	长沙
西北地区	西安	拉萨
	兰州	乌鲁木齐
华东及华中地区	南京	南昌
	上海	
	武汉	合肥

杭州安恒信息技术股份有限公司
DBAPPSecurity Co., Ltd.

官网： www.dbappsecurity.com.cn
电邮： info@dbappsecurity.com.cn
客服热线： +86-400-6059-110
直通专线： 首席客户成功官 沈亚婷 18100188999
首席客户成功官 刘蓝岭 18100189888

安恒官方微信

杭州总部

地址： 杭州市滨江区西兴街道联慧街188号安恒大厦
座机： +86-571-88380999/28860999
传真： +86-571-28863666

科创板：688023

安恒信息
DAS-security 安全中国

科创板：688023

明御®
安全网关（下一代防火墙）

全流程防御｜云管端防护｜安全可视

杭州安恒信息技术股份有限公司
DBAPPSecurity Co., Ltd.

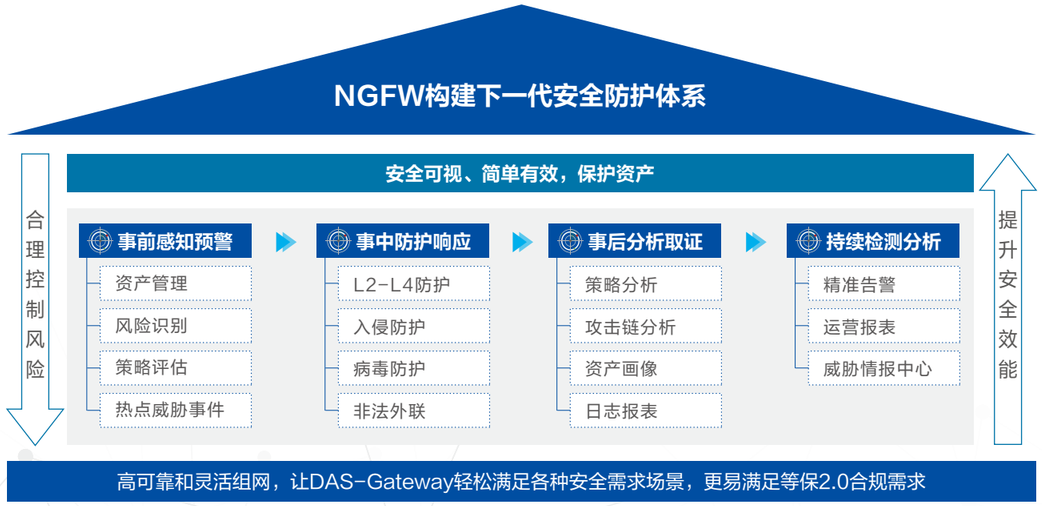
安全背景

网络信息技术为企业运营提供了有力支撑，企业也越来越依赖网络，但同时网络上的黑客攻击、蠕虫病毒传播、非法渗透等，严重影响企业信息系统的正常运行。采用防火墙部署在网络边界是当前防护企业网络安全的主要方式，但是当前防火墙普遍存在着以下问题：

- **问题一：防护流程不完善**
  传统信息安全建设，以事中防御为主，缺乏事前预防和事后分析取证的闭环安全保障能力。
- **问题二：未知威胁、0day攻击让企业防不胜防**
  防火墙通常基于特征实现威胁检测和阻拦，该方法无法对未知威胁、0day攻击进行及时检测。
- **问题三：访问控制策略繁杂、管理困难**
  防火墙的核心功能依然是访问控制，而40%的安全事件均因访问控制策略配置不当导致。
- **问题四：安全日志难以联动分析**
  防火墙安全日志种类和安全威胁类型繁多，且不能结合业务形成有效的安全状态分析。

产品概述

安恒信息明御®安全网关（以下简称“NGFW”）秉持安全可视、简单有效的理念，以资产为视角，构建“事前+事中+事后”全流程防御的下一代安全防护体系，并融合传统防火墙、入侵防御系统、防病毒网关、上网行为管控、VPN网关、威胁情报等安全模块于一体的智慧化安全网关。



产品功能

功能	描述
网络特性	• NAT及ALG • 支持链路负载均衡、服务器负载均衡 • 满足IPv4/IPv6双栈环境 • 支持4G接入，在4G接口上运行IPsecVPN
访问控制	• 支持基于多元组的访问控制 • 提供策略分析引擎，可分析冗余策略、隐藏策略、冲突策略、可合并策略、空策略、过期策略等问题策略
资产发现	• 支持主动和被动方式从网络流量中发现识别资产，获取资产基本信息
用户认证	• 支持Web认证，微信认证、短信认证、免认证等多种认证方式 • 支持AD域单点登录
应用管控	• 支持主流P2P、IM、在线视频、网络游戏、网络炒股等应用识别 • 提供应用管控，支持针对应用动作、应用内容的细粒度控制 • 支持多种应用特征规则，可提供在线升级和手动升级
URL过滤	• 支持自定义URL过滤 • 支持识别恶意网站、违法网站 • 千万级URL特征库，可提供在线升级和手动升级
流量控制	• 支持通道化的QoS，基于地址、用户、服务、应用、时间进行带宽控制 • 对多层级通道进行最大带宽、保障带宽、每IP或每用户的限速 • 基于优先级的差异性服务，支持带宽均分策略 • 支持日流量限额、时长限额 • 支持流量惩罚通道和限速通道
网络攻击防护	• 支持对ARP攻击、多种异常报文攻击的防护 • 支持扫描攻击防御 • 支持对SYN Flood、DNS Flood等多种DoS/DDoS攻击的防护

功能	描述
入侵防御	• 支持针对HTTP、IMAP、NETBIOS等多种协议和应用的攻击检测和防御 • 支持预定义防御配置模板，自定义入侵防御特征 • 支持IPS高阶告警功能 • 支持基于多种特征的攻击检测和防御，可提供在线升级和手动升级
病毒防护	• 支持对多种文件格式的病毒文件扫描 • 支持对HTTP、FTP、IMAP、POP3、SMTP协议病毒的查杀 • 支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型的病毒 • 超过百万的病毒特征库，可提供在线升级和手动升级
威胁情报	• 支持全网威胁情报的搜索查询 • 支持热点威胁情报订阅，并提供配置向导协助管理员生成安全防护策略 • 支持威胁情报关联本地资产进行威胁持续检测分析
攻击链分析	• 支持整合安全日志进行链式分析 • 支持以攻击者、被攻击者的视角进行安全事件展示
VPN	• 支持SSL VPN、IPSec、GRE等多种VPN • 支持IPSec VPN第三方对接及IPSec VPN快速配置 • 支持国密算法
高可用性（HA）	• 主主模式和主备模式 • 支持配置、会话、特征库、IPSec VPN状态同步
日志报表	• 支持本地日志记录和远程日志输出 • 支持专用的日志审计管理软件 • 支持预定义、自定义统计报表模板

产品特点

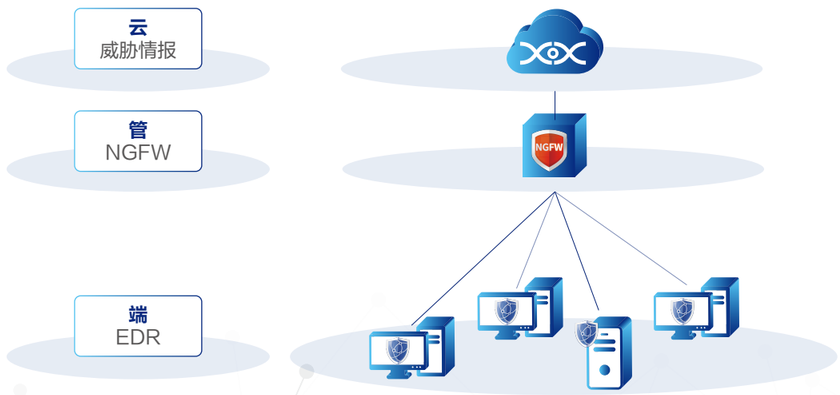
全流程防御体系

明御®安全网关构建“事前+事中+事后”全流程防御的下一代安全防护体系，从被动防御的安全体系向事前预防、事中响应、事后审计的动态保障体系转变，帮助企业大幅度降低安全事件产生的不良影响。

云管端立体式防护

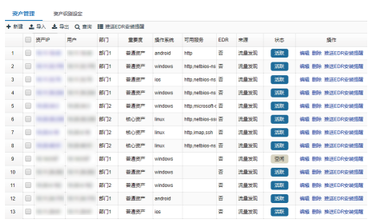
明御®安全网关支持与云端的威胁情报联动，获取海量情报信息，并利用威胁情报分析内网资产安全情况，可以快速发现内网未知威胁、0day攻击等，准确发现内部失陷主机，掌握威胁根源，从而帮助用户提前做好安全防范、快速进行攻击检测与响应；还支持与终端的EDR联动，通过NGFW的边界部署位置的优势+EDR推广策略的功能，实现对终端的网络准入认证控制。并且在EDR的主机安全防护助力下，规避防火墙的终端防护能力不足的现状。

明御®安全网关与威胁情报、EDR的联动，打造了“云+管+端”的立体式防护架构，为用户提供持续有效的边界防护、保障主机安全，形成安全闭环。

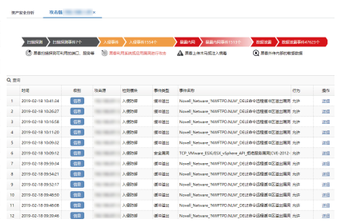


安全可视化

明御®安全网关采用主动扫描和监控主机流量等方式识别网络中的资产信息，把难以分析的安全日志以资产为视角按照攻防逻辑，把攻击者入侵分为前期阶段、尝试阶段、渗透阶段、外传阶段，编排成攻击链，让普通网络管理员也能进行安全分析，明确感知到安全事件的严重性；同时，明御安全网关也支持把难以关联的审计日志以用户为视角进行关联分析，方便对网络主体中的“人”进行风险控制和业务优化。



资产识别

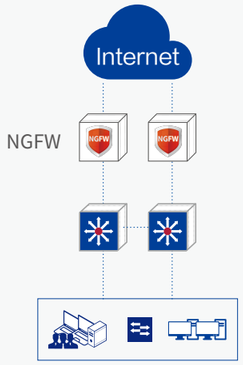


攻击链分析

资产画像

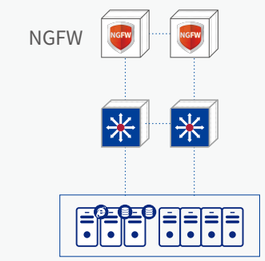
应用场景

互联网出口防护



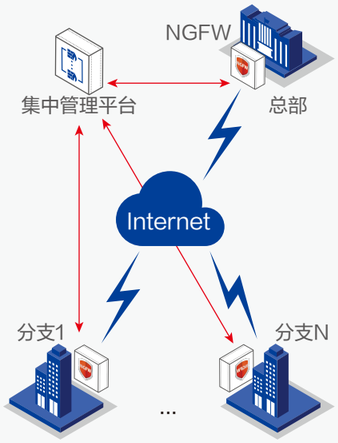
- **出 口 特 性：** 通过链路负载均衡、NAT、链路探测等出口特性功能，实现多个ISP出口的智能路选
- **访 问 控 制：** 基于多维度的访问控制，实现内外网隔离；提供策略分析引擎，保证访问控制规则数量最小化
- **安 全 防 护：** 提供入侵防御、病毒防护、恶意URL过滤等功能防止外界利用漏洞进行入侵、以及僵尸、木马、病毒、恶意代码入侵
- **威 胁 情 报：** 威胁情报发现未知威胁、0day攻击等，提供持续检测分析能力
- **流 量 管 理：** 弹性QoS优化，保障重要业务的同时让出口更通畅
- **安 全 可 视：** 自动识别内网资产情况，并提供以资产维度的安全智能可视化分析，便于管理员分析取证溯源

边界防护



- **资 产 管 理：** 自动识别内网资产情况，构建对IT资产实现多维度的安全分析监控
- **访 问 控 制：** 实现不同区域隔离；并提供策略分析引擎，协助管理员删除多余或无效的访问控制规则，满足等保2.0对控制规则数量最小化要求
- **安 全 防 护：** 提供入侵防御、病毒防护、恶意URL过滤等功能防止外界利用漏洞进行入侵、以及僵尸、木马、病毒、恶意代码入侵
- **非法外联防护：** 检测服务器是否有主动外联行为，可尽早发现C2C，信息外泄问题，并实时阻断
- **威 胁 情 报：** 威胁情报发现未知威胁、0day攻击等，提供持续检测分析能力
- **安 全 可 视：** 自动识别内网资产情况，并提供以资产维度的安全智能可视化分析，便于管理员分析取证溯源

分支组网



- **访 问 控 制：** 本端的内外网隔离，各分支VPN组网流量的精细控制；并提供策略分析引擎，协助管理员优化访问控制列表
- **上网行为管理：** 支持多种认证方式，屏蔽高带宽消耗应用，限制敏感信息的外传，禁止对钓鱼网站的访问
- **安 全 防 护：** 提供入侵防御、病毒防护、恶意URL过滤等功能防止外界利用漏洞进行入侵、以及僵尸、木马、病毒、恶意代码入侵
- **威 胁 情 报：** 威胁情报发现未知威胁、0day攻击等，提供持续检测分析能力
- **安 全 互 联：** 支持IPSec和SSLVPN；IPsec VPN与业界主流厂商对接案例丰富；快易IPsec VPN，业务变化自动收敛，分支极简运维
- **集 中 管 理：** 集中管理平台实现总部、分支多台设备的统一运维管理