融讯光通
RONG XUN GUANG TONG

网络安全系列产品彩页

拟态防火墙

产品概述

2016 年 4 月，习近平总书记在网络安全和信息化工作座谈会上指出“网络安全的本质是对抗，对抗的本质是攻防两端能力的较量”。

公安部牵头，一年一次，组织攻防两方，进攻方将对防守方发动网络攻击，检测出防守方存在的安全漏洞：

2016 年公安部、民航局、国家电网三个事业单位参与“HW2016”行动

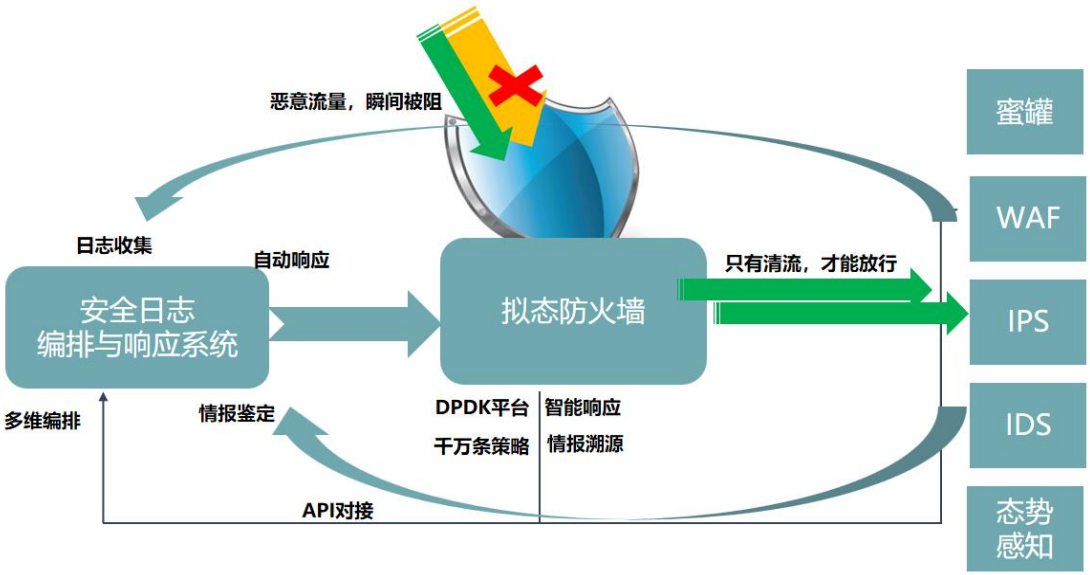
2017 年部分政府部门加入“HW2017”行动

2018 年部分国有企事业单位及其它重点单位加入“HW2018”行动

2019 年工信、安全、武警、交通、铁路、民航、能源、新闻广电、电信运营商等单位都加入到“HW2019”行动

2020、2021 年，护网已经成为常态

产品特性



- 主动防御架构：通过构建动态变化的网络迷宫来增加攻击成本和代价，使攻击者无法定位和预测目标，从而降低威胁发生的概率；打造的网络迷宫具备不确定性、迷惑性和欺骗性等特性，大幅提升了网络自身的对抗能力和防御能力，扭转了传统网络防御天生被动的态势，实现了从被动到主动、从静态到动态的突破。
- 动态 IP 封堵：通过多源威胁情报进行实时信誉鉴定，按照 IP 信誉进行实时阻断，可针对威胁 IP 进行一键溯源；通过某一个应用系统的威胁攻击行为，直接在整个数据中心上进行全面防御

做到实时阻断；做到分钟级封堵攻击者的 IP 资源，可有效打击黑客攻击及演练攻击的团伙行为及 IP 资源。

- 网络防护第一道关口，解决防火墙无法应对规模威胁 IP 攻击问题！
- 动态情报更新，以及 Bypass 功能，让拟态防火墙在 HW 之外也能防护网络安全。

产品功能

- 实时监控：实时学习保护网络状态，监控外网异常行为，发出警报，自动处置。
- 全息伪装：利用空余网络资源，构建全息哨兵节点，监控异常行为，迷惑和诱捕攻击者。
- 端口虚开：针对真实业务主机虚拟开放敏感端口，诱使攻击者对虚开端口发起攻击。
- 黑白名单：支持设置黑、白名单，来防止自由网络地址及业务服务器地址被误拦截。
- 封堵国家地区：支持按照国家及地区来一键封堵该国家区域的网络访问，同时也进行该数据中心访问该国家地区的网络地址。
- 日志溯源：支持网络的全量网络五元组信息及网络协议的查询溯源，且还支持国家地区进行搜索查询。

主机 EDR&CWPP

产品概述

随着云计算、大数据技术的发展，大量的业务都集中在网络中，那么数据中心的业务安全性以及可靠性将至关重要。除了在边界防护外，如何将安全和可靠性后移，保证核心主机上关键业务的安全和高可靠性变得尤为重要。

融讯光通以 EDR 端点检测与响应技术理念为核心，结合 CWPP、微隔离、自适应安全等前沿技术，能实时检测未知威胁并快速响应。广泛部署于安装了 Windows、Linux、国产操作系统的服务器、云主机、工控主机等泛在行业主机。

产品功能

风险发现

可自动识别系统内部资产情况，并与风险和入侵事件自动关联，提供灵活高效的回溯能力，帮助企业资产可视化。

- 主机发现：通过设置检查规则，系统自动检查已安装探针主机，所在网络空间未纳入安全管理的主机，自动排除普通网络设备:保证探测与被探测主机正常运转。
- 应用清点：自动化清点中间件、数据库、大数据组件 Web 应用、Web 框架、Web 站点等资产;根据每个服务器业务特点，针对性地识别别应用 200 余类。

- 资产快速检索：对于每类业务资产，系统提供”主机视角“和”资产视角“两种通用维度，聚合展示数据，客户可灵活定义自己的表格显示;关键资产（主机账号，进程等)全系统关联。
- 资产面板：在获得资产信息后，将结合业务情况形成“概览视图”与“分级视图”，展示企业整体资产状况,多维度剖析单一资产，详细分析内部情况;引导客户从安全维度发现一些问题。

入侵检测

可实时对黑客的入侵行为进行检测及实时监控告警、处理发现入侵事件，提供快速防御和响应能力。

- Web 后门检测：通过自动化地监控关键路径，结合正则库，相似度匹配，沙箱等多种检测方法，实时感知文件变化，从而能够及时发现 Web 后门，并对后门影响部分进行清晰标注。
- 反弹 shell：通过对用户进程行为进行实时监控，结合行为的识别方法，及时发现进程的非法 Shell 连接操作产生的反弹 Shell 行为，有效感知知 0day 漏洞利用的行为痕迹，并提供反弹 Shell 的详细进程树。
- 本地提权：通过对用户进程行为进行实时监控，结合行为识别技术，我们能及时发现进程的提权操作并通知用户，并提供提权操作的详细信息。
- 系统后门监控：通过对进程关联信息的分析，结合模式识别和行为检测，提供不依赖 Hash 的自动化系统后门检测方式，实现在多系统中进行多维度、高准度、快速度的后门发现。

合规基线

构建了由国内信息安全等级保护要求和CIS组成的基准要求，帮助用户快速进行企业内部风险自测，发现问题并及时修复，有助于您更好的管理服务器基线安全。

- 支持等保 2.0/CIS 等多重标准：安全研究人员持续研究国家等级保护政策、CIS 基线标准，不断推进更多基线标准的支持。产品目前支持 Centos、Debian、RedHat、Windows、Ubuntu 等常用操作系统。
- 自动识别服务器需检查的基线：在资产细粒度清点的基础上，根据所选服务器的操作系统、软件应用等信息，自动筛选出该服务器上需要检查的系统、应用基线。同时支持一键批量创建其线任务操作简单易用。
- 一键任务化检测，结果可视化呈现：合规基线功能设计了灵活可配置的任务式的扫描机制。用户可快捷创建其线扫描任务，根据检测需要自行选择需要扫描的主机和基线，检测完成后，基线检查结果将分为检查项视图和主机视图可视化呈现。
- 开放企业自定义基线检查项能力：企业可根据实际的使用场景，自行定义基线的检查项，如定义检查闭值、自定义检查目录、自定义检查结果展现模板、自定义检查项整改方案等等，以满足企业多样化的内部监管要求。

产品优势

- 轻量 Agent：Agent 占用资源极少，不影响主机系统的正常运行。
- 内集中管理：实现检测和防护的一体化管控，降低管理的难度和复杂度。
- 全面防护：提供事前预防、事中防御、事后检测的全面防护，全面降低入侵风险。
- 完善的事件审计：完整记录保存安全事件的日志信息，方便用户进行安全事件审计，并可灵活设置安全事件的告誉规则。

优势特点

我司安全探针与传统主机安全产品对系统资源占用对比图：

类别	传统主机安全产品	我司主机安全产品 优
安装包	大-350M	小-10M
CPU占用	高-10%	低-1%
内存占用	高-120M	低-25M
兼容性	不能与其他安全软件共存	可与其他安全软件兼容
检测方式	全盘文件扫描，特征库比对	操作系统定点监控，行为合规监控，横向比对“找不同”
安装及维护	用户+管理员	管理员

应用场景

入侵检测和资产清点

融讯光通
RONG XUN GUANG TONG

漏洞检测和基线检测

工业控制主机安全

融讯光通
RONG XUN GUANG TONG

漏洞扫描

产品概述

融讯光通漏洞扫描系统是一款可以高效、全方位检测网络中各类脆弱性风险的产品，内置多种扫描引擎，从系统漏洞、数据库漏洞、Web 漏洞、弱口令风险、基线配置等多角度进行信息资产的脆弱性审计，提供专业的安全分析和修补建议，并能够与防火墙、态势感知等系统联动形成综合防护方案，全面提升信息系统的安全性。

产品特性

全面资产识别

- 掌握资产状态，摸清资产风险情况，提高风险应对能力，全面检测各类网络资产的脆弱性隐患。

丰富知识库

- 海量漏洞库涵盖国产化系统、云计算平台、大数据组件、物联网等多种类型漏洞，内置全面的基线核查知识库。

直观可视化展示

- 漏洞趋势、漏洞类型图形化展示，安全风险一目了然，提供简洁直观的风险解决方案，帮助用户快速解决安全隐患。

完善扫描能力

- 支持基线核查、系统扫描、Web 扫描、数据库扫描、弱口令检测等多种扫描任务，适用多种环境。

高效协同防护

- 支持与防火墙协同防护，提高风险处置能力，对接态势感知系统，接收态势感知系统下发任务，提供安全分析依据。

灵活部署方案

- 支持独立式部署、分布式部署，支持 VMware、KVM、Openstack 等云环境部署，支持 IPv4 和 IPv6 环境的部署。

融讯光通
RONG XUN GUANG TONG

应用场景

等保合规

- 等保 2.0 中明确要求：“应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补”。
- 定期的网络安全自我检测、评估，帮助客户满足合规性要求。
- 精准识别网络资产，感知资产风险变动、有效管理资产。
- 提供丰富全面的规则库，高效发现脆弱性威胁，并提供检测报告和修复建议。

业务上线检测

- 在应用系统（业务系统）正式投入生产运行之前，对其进行全方位的安全检查，提前消除安全隐患，降低漏洞修复成本，保障系统稳定运行。
- 采用 IAST 技术实现安全左移，降低漏洞修复成本。
- 操作简单去专业化，开发测试人员皆能轻松使用。
- 极低误报及漏报，提供专业的漏洞检测报告和修复建议。

突发漏洞排查

- 面对突发漏洞事件时，24 小时内提供应急响应，能够第一时间实现快速的漏洞影响范围评估，指导客户修复或临时下线受影响资产，最大程度降低客户损失。
- 24 小时内提供应急响应，降低客户资产受侵害空窗期。
- 全面、快速、精准识别信息资产，第一时间定位漏洞影响范围。
- 提供清晰明了的报告和修复建议，指导客户及时消除风险。

客户价值

满足合规监管要求

- 拥有全面、快速、精准的扫描能力，及时发现安全漏洞和隐患，并提供简洁明了的修复指导，帮助客户满足各类合规检查、监管检查要求。

提高漏洞管理水平

- 对漏洞信息进行动态管理，提供漏洞发现、评估、分析、验证、复核的全生命周期管理，实现对漏洞风险管理的整体闭环。

提升漏洞响应能力

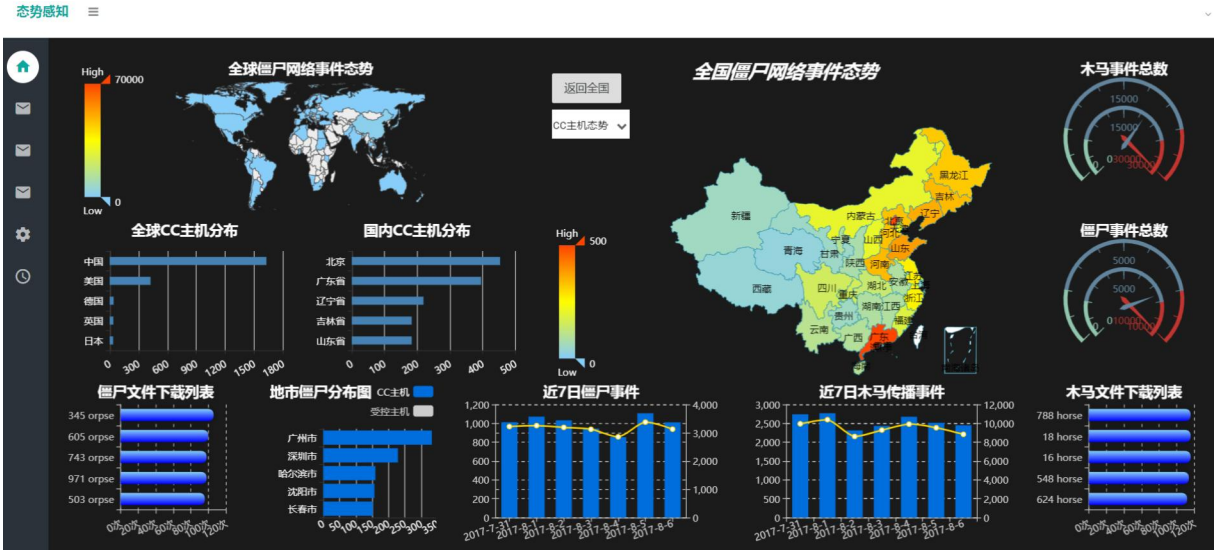
- 实现突发紧急漏洞应急支持，24 小时内提供漏洞排查插件，指导客户修复或临时下线受影响资产，最大程度降低客户损失。

融讯光通
RONG XUN GUANG TONG

大数据态势感知

产品概述

融讯光通大数据态势感知系统是一款功能强大的安全解决方案，通过收集和监测各种安全相关数据，利用机器学习和数据分析技术，实时识别和分析潜在的安全威胁，并以可视化的方式展示安全态势，帮助安全团队及时响应和处理安全事件。



产品功能

- 安全运维门户：安全运维工作集中入口，实现安全态势展现与工作集中管理。
- 数据采集：采用大数据技术实现数据采集、数据存储、数据处理功能。
- 安全知识库：包括指标库、模型库、场景库、风险库、规范标准等知识。
- 智能感知：智能分析识别高危事件和潜在风险，并形成告警。
- 安全预警管理：基于系统脆弱性、风险评估结果，产生预警与报警。
- 安全风险管理：赋值计算，实现风险量化，支持风险整改追踪等工作。
- 安全合规管理：管理和技术上的平台化、体系化、集中化合规管理体系。
- 安全运维管理：第三方系统集成，组成全面的、整体联动的安全管理平台。
- 安全报告中心：提供多维度，可自定义组合条件查询的综合安全报告中心。

产品价值

为 IT 系统建立一套重要的安全保障的生产系统

建立您的预警-防护-应急处置机制实现：

- 实时预警遭受的安全问题（如黑客攻击、病毒、挂马、非法用户入侵等）；

- 提供相应的安全防护工具和解决方案，对 IT 系统进行经常性的安全检查，及时发现出现的各种安全隐患；
- 提供事后的应急处置预案和向导。

实现 IT 系统的顶层防护

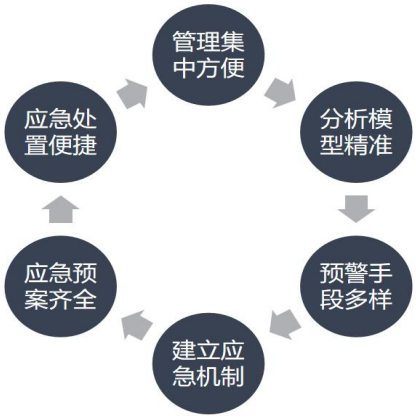
- 在系统遭受大面积攻击危害系统安全时,天鹰网络与应用安全预警处置平台“可针对攻击手段提供相应的防护解决方案以及应急处置预案，及时解决您的系统安全问题，并分析安全运行状况，采取相应的措施，消除日后的安全隐患。

提高网络与信息安全事件应急处置能力

- 根据应急预案规范流程，科学、有效的处理各类安全事件，健全应急响应处理机制，提高应急处置效率。

主要优势

- 通用大数据 hadoop 发布版本的稳定性增强技术
- 高性能的安全业务处理平台，ES 处理性能，单机 2 万条/秒（单台普通服务器提供 hadoop）
- 新增的特色业务流程：地理位置富集
- 本地化、客户友好的显示界面
- 电信级的 CC 溯源系统
- 高集成，可实现单台设备的大数据态势感知



融讯光通
RONG XUN GUANG TONG

系统架构

可视化层
- 基于NoSQL中的分析结论、ES上的全文检索文件，提供检索、报表、态势视图可视化功能。
- 提供接口对各类安全子系统及功能模块进行集成

分析计算层
- 基于Spark Mllib、mahout中的经典算法实现，以及自定义开发MapReduce程序及hive的类sql接口进行分析计算，分析的结论、报告统计结果等存储在NoSQL中。

数据存储层
- HDFS、ElasticSearch、Hbase、RMDBs

数据处理层
- 数据库中间件：Kafka，作为消息协同中间处理层
- 数据处理：Storm、Storm Streaming、ETL数据清洗

数据采集层
- 支持Flume-ng、Sqoop、爬虫及logmanager采集器
- 支持Syslog、SNMP、FTP、SSH、JDBC、Robot等采集协议

数据源
- 内部数据：基础设施、安全设备、终端、业务系统各类日志
- 外部数据：外部威胁情报、互联网接口数据、合作方数据