华为乾坤安全云服务技术主打胶片

Security Level:

HUAWEI

目录

1. 企业网络安全建设面临的挑战
2. 华为乾坤安全云服务
3. 成功案例

HUAWEI

网络安全建设的三大核心目标：

防护有效果

安全能力全面

安全威胁精准识别

威胁发生及时隔离阻断

（全面、精准、及时阻断）

运维要简单

交付简单、快速

日常运维成本降低

应急服务及时、有效

（快速、有效、降低OPEX）

投资收益平衡

安全产品防护能力强

运维效果好

驻场服务快速闭环安全问题

（防护强、效果好、快速闭环）

安全产品堆砌、运维短板、防御效果不佳，企业安全建设困扰繁多

防御效果差

2019.5易到用车被巨额勒索

- **关键告警被淹没**

大量低价值安全告警，淹没有效安全事件，威胁无法及时处置

- **缺乏全局统筹**

单产品孤立的威胁分析，难以做到全局统筹，无法准确识别威胁

专业运维缺失

2020年我国信息安全人才缺口140万

- **运维人才短缺**

网络设备发挥效应依赖专业运维人员，专业人员养不起、留不住

- **安全驻场难确保**

购买驻场安全服务，人员能力参差不齐、无法确保防御效果

产品堆砌投资大

2020年中国网络安全市场总体支出将达到87.5亿美元

来源：IDC中国，2020

- **安全产品堆砌**

企业网络安全的全面建设，需要十几种甚至几十种安全产品和方案

- **高投资**

大量安全产品的堆砌，大幅提升网络安全建设投资成本

HUAWEI

顺应网络安全建设的发展趋势，安全运营方式也在不断改变

传统运营方式

安全产品组合 + **自行运维**

安全产品种类多，运维人员缺口大，专业性无法保证，导致安全产品防御能力不能100%发挥

- 产品种类多，各自为战
- 极少登录查看日志、优化策略
- 业务方抱怨先于安全日志发现
- 7*24被动应急，基于网上指引

安全产品组合 + **安全驻场**

安全产品组合，组件良莠不齐；驻场服务人员能力参差不齐，前后端联动效率低，难以达到安全实效。

- 产品种类多，良莠不齐
- 5*8安全运维，部分日志分析
- 主动发现部分安全问题
- 7*24被动应急，基于远程指导

可管理安全服务

采集/阻断设备 + **云端服务**

专业安全能力平台化，技能储备强、实操经验足的专家运维，借助云端平台实现高效服务交付

- 安全能力平台化，按需购买
- 7*24安全运维，全量日志分析
- 主动发现基于流量全量安全问题
- 7*24主动应急，威胁情报触发

Gartner:

- **可管理安全服务：** “对安全事件和与安全相关的数据源的远程监视，或者对IT安全技术的管理以及与安全事件监视一起通过远程安全运营中心（SOC）的共享服务来提供，而不是通过一对一地交付给单个客户的现场或远程服务人员。”
- 可管理安全服务的全球市场在2019年增长了**7.5%**，收入达到了**115亿**美元。在新兴服务的推动下，市场表现比上年更好。

传统安全方案无法适配广众用户诉求，安全云服务创新模式成为优选

AS IS：业界传统安全方案

传统安全方案：线下软硬件安全产品+周期性安全服务+安全驻场服务

劣势：

- 产品、服务交付形式重载，投入大；
- 运维人员缺乏、驻场服务人员能力参差不齐，运维难度大；
- 各局点安全防护各自为战，缺乏全局统筹，防御效果不佳。

本地现场交付三级等保安全方案及服务

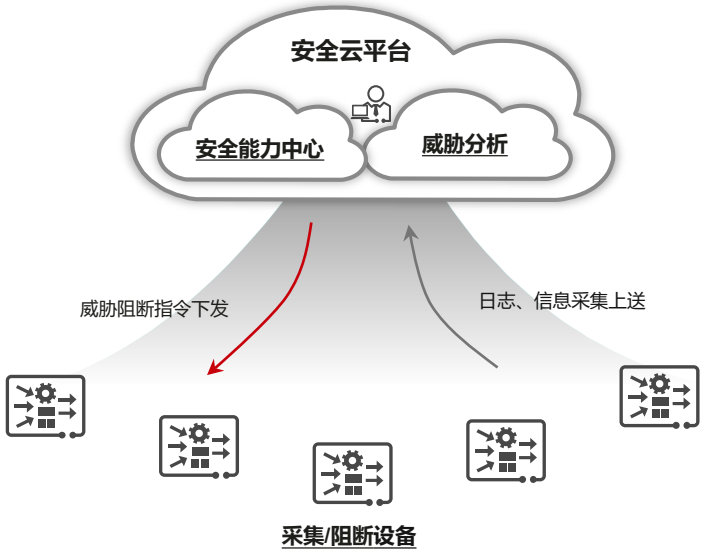
To Be：安全云服务

安全云服务：云端安全能力中心/分析+本地执行器/采集器

优势：

- 云边一体化新架构，产品、服务交付云化提供；
- 云端专家替代本地运维，7*24小时在线服务，简化运维难度；
- 资源、信息全局共享，防御效果提升。

安全云服务



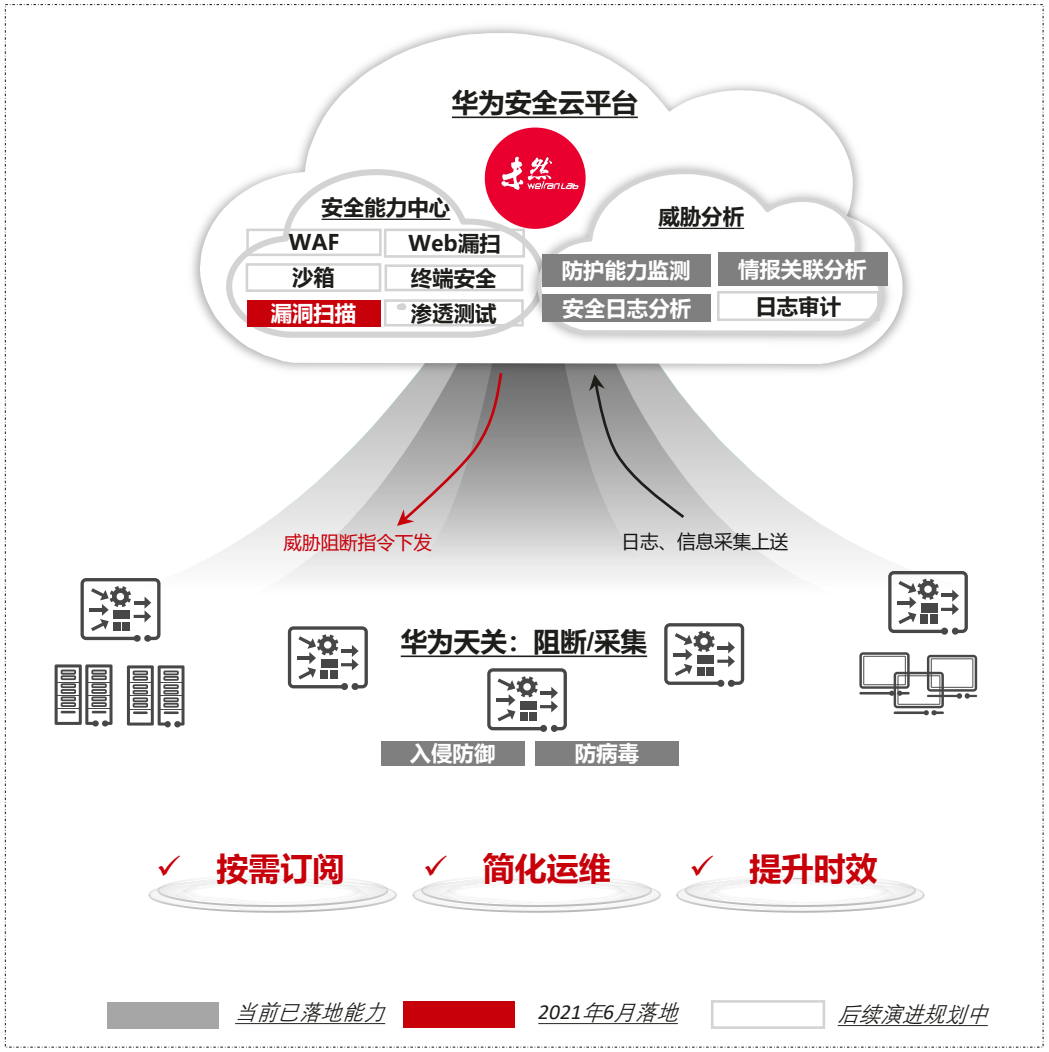
目录

1. 企业网络安全建设面临的困扰

2. 华为乾坤安全云服务

3. 成功案例

华为乾坤安全云服务：创新云边一体架构，打造一站式安全云服务



乾坤：打造网络空间朗朗乾坤

乾坤取义天地。乾为天，坤为地，华为乾坤安全云服务通过云端、本地融合的创新技术架构，打造简单高效、安全可靠的安全服务全新模式。

乾：华为安全云平台

华为安全云平台：安全能力中心+威胁分析+云端专家服务

核心功能

1.安全能力中心：提供平台能力，后续持续增加日志审计、态势感知、漏洞扫描等安全能力

2.威胁分析：基于智能技术对安全日志和取证文件关联分析，准确、快速处置攻击事件；

3. 云端专家服务：具备攻防对抗经验的未然实验室安全专家，7*24小时在线服务

坤：华为天关

华为天关：采集+阻断

核心功能

1.采集：采集并发送安全日志通过加密通道发送至华为安全云平台，为威胁分析提供数据；

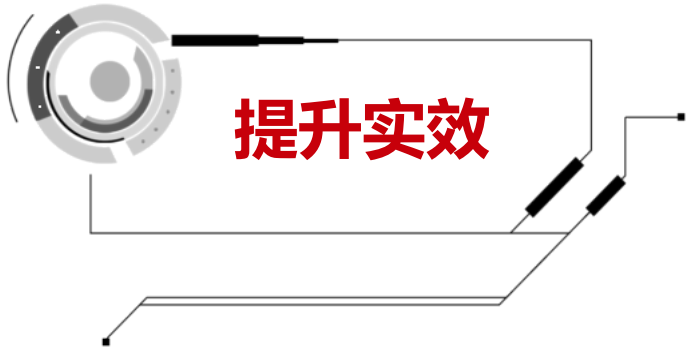
2.阻断：对网络中的流量数据进行深度安全检测，发现并阻拦攻击流量及恶意文件；接收云端下发的黑名单信息，执行IP封禁动作。

HUAWEI

华为乾坤安全云服务，打造网络安全空间朗朗乾坤

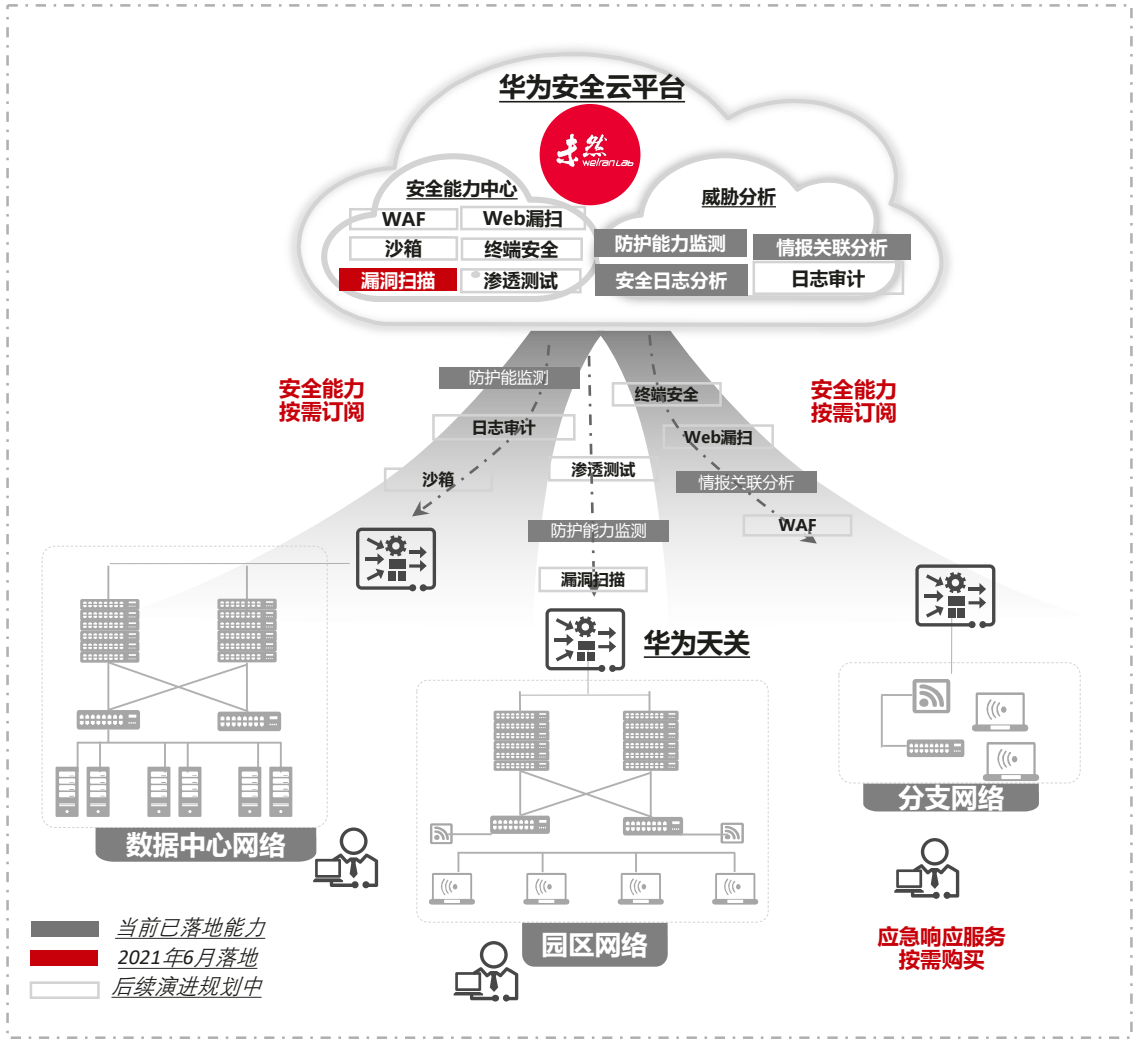
- 安全云服务，云端提供多种安全能力按需订阅，只需要很少的安全投资，即可完全替代在本地部署多种传统安全产品

- 云端专家+智能替代本地运维人员，专家解决“疑难杂症”，利用大数据智能分析提升自动运维效率，提供7x24小时在线服务，减少了本地运维工作量，简化了运维难度



- 云端专家深入攻防对抗过程，整合安全能力，解决“疑难杂症”，云端自动应对业界最新漏洞与攻击方法，一处发现威胁，全局快速免疫

按需订阅：全面安全能力+应急响应按需购买，适用于各类安全场景



华为云基础+高品质安全能力，打造安全能力平台

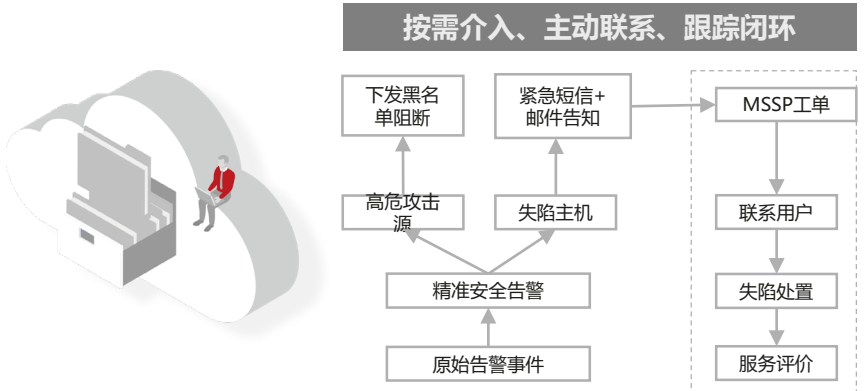
华为云：三级等保保障，合规授权，保障隐私

AV：智能技术赋能恶意文件检测，检出率97%

未知威胁：基于智能技术进行失陷主机检测，切断控制端，准确率99%

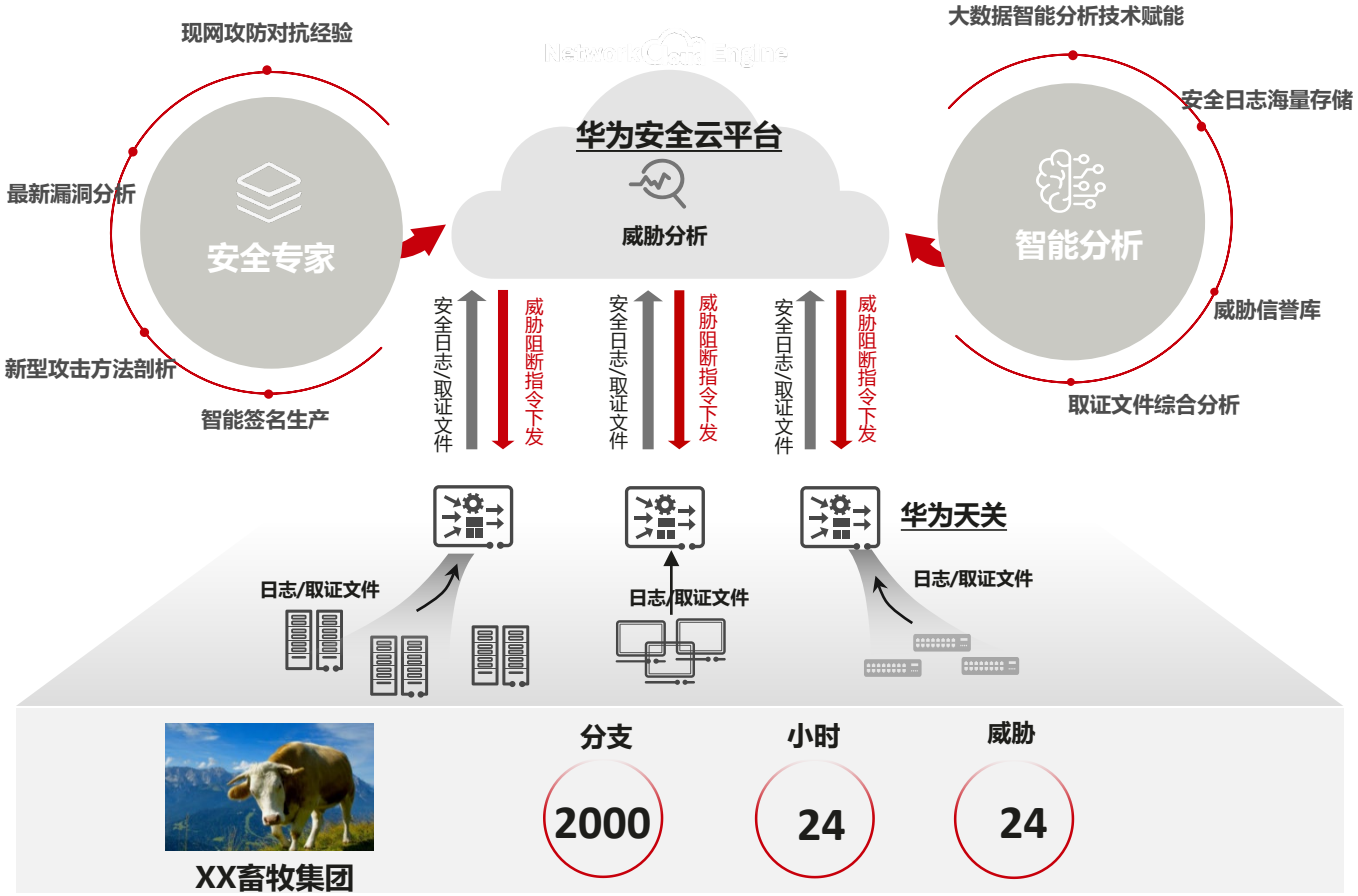
IPS：12000+签名，默认阻断率80%

按需购买，及时响应，追踪闭环



HUAWEI

提升实效：攻防经验提升云端安全能力+智能关联分析，精准识别威胁及时处置



攻防经验提升云端安全能力

- 专家现网攻防对抗经验固化到云端，不断增强云端安全能力
- 最新漏洞分析、新型攻击方法剖析、云端智能签名生产，快速应对新型攻击
- 具备攻防对抗经验的运维专家，可以运用云端各种安全能力，解决最新“疑难杂症”

关联分析增强全局免疫

- 全局统筹，基于对安全日志和取证文件进行关联分析，降噪处理，精准识别有效攻击事件
- 全面的威胁信誉库，基于华为安全能力中心、未然实验室信息收集、本地天关有效分析结果汇总等多种途径，不断增强
- 威胁信息全局共享，一处检出，全局快速免疫
- 提升自动运维效率，自动拦截攻击，响应效率由小时级提升至分钟级

简化运维：云端安全专家替代本地运维，安全态势多维度全面感知

云端共享安全专家资源7*24小时在线服务

周期性周报/月报

- 按周、按月提供安全报告，邮件主动推送，全面掌握网络安全态势；

紧急短信告警

- 安全事件被分级、分类、降噪处理，紧急事件通过短信和邮件立即通知，指导用户进行及时安全处置；

手机APP全局态势感知

- App随时检查网络安全态势评分、设备运行状态、威胁和风险概览，处置安全事件
  -*2021年3月发布*

HUAWEI

目录

1. 企业网络安全建设面临的困扰

2. 华为乾坤安全云服务

3. 成功案例

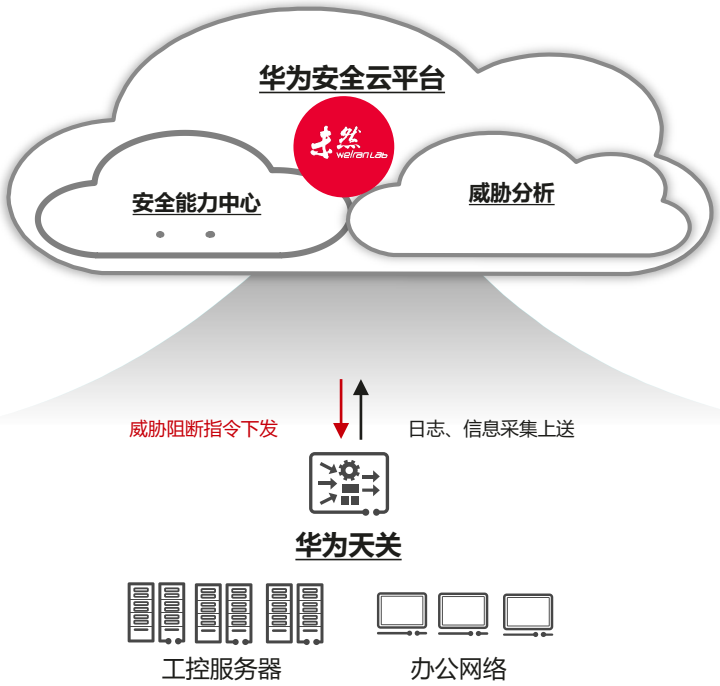
乾坤安全云服务，为制造业重构网络安全建设思路

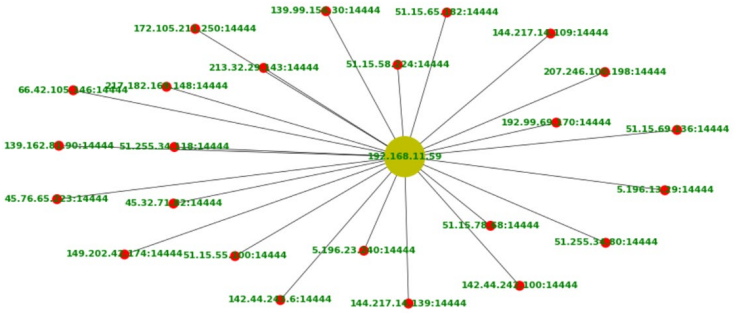
中国某轮毂制造商

- 工控服务器负载超荷：服务器负载超过预期，生产风险高
- 大量终端行为失控：发现大量外联行为，信息外传风险大
- 运维人员不堪重负：每日百计安全日志，人工处理负担重

- 内部失陷主机难以识别，产线存在安全风险
- 专业运维人员缺乏，现网安全设备无法发挥作用
- 安全产品投资大

方案架构





内网一工控服务器外联矿池情况

客户价值

系统上线24小时后，效果明显

96台

- 发现126台主机失陷，存在挖矿行为，消耗主机生产性能

21万次

- 阻断21.8W次挖矿相关恶意行为

95%

- 降低运维人员95%工作量，轻松运维

HUAWEI

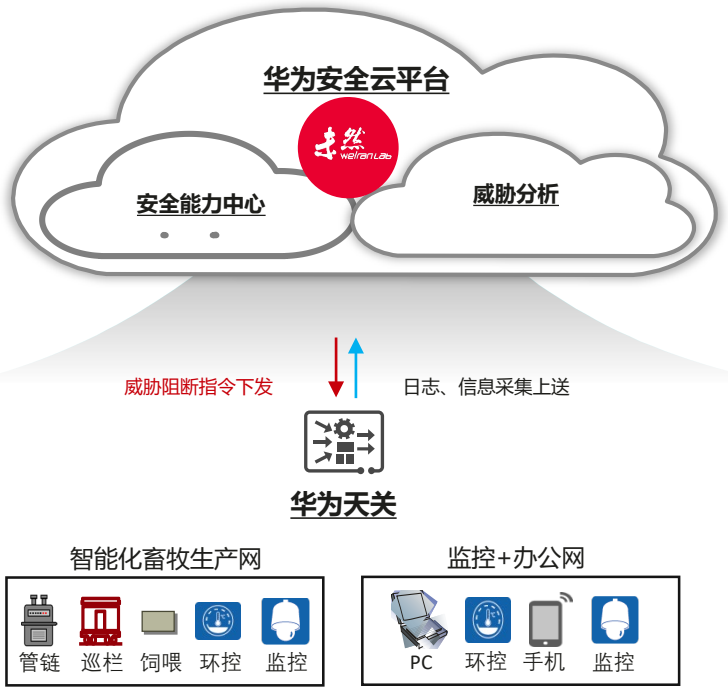
乾坤安全云服务，为畜牧业生产保驾护航

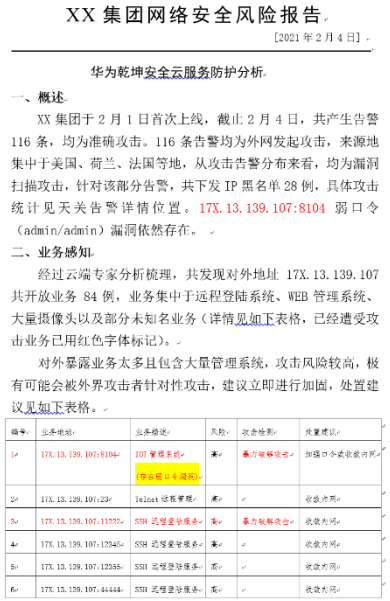
中国某畜牧业集团

- 服务器遭攻击：无法分析风险，只能直接下线业务
- 业务复杂：对外提供网络业务多，安全风险不可知
- 运维覆盖难：X个厂区共享1个运维人员，设备运维力不从心

- 生产流量复杂，传统方案识别能力不足
- 安全事件处置慢，防护实效有限
- 运维人员安全能力有限，人员覆盖不足，只能被动相应

方案架构





XX 集团网络安全风险报告

[2021 年 2 月 4 日]

华为乾坤安全云服务防护分析

一、概述

XX 集团于 2 月 1 日首次上线，截止 2 月 4 日，共产生告警 116 条，均为准确攻击。116 条告警均为外网发起攻击，来源地集中于美国、荷兰、法国等地，从攻击告警分布来看，均为漏洞扫描攻击，针对该部分告警，共下发 IP 黑名单 28 例，具体攻击统计见天关告警详情位置。17X.13.139.107:8104 弱口令（admin/admin）漏洞依然存在。

二、业务感知

经过云端专家分析梳理，共发现对外地址 17X.13.139.107 共开放业务 84 例，业务集中于远程登陆系统、WEB 管理系统、大量摄像头以及部分未知名业务（详情见如下表格，已经遭受攻击业务已用红色字体标记）。

对外暴露业务太多且包含大量管理系统，攻击风险较高，极有可能会被外界攻击者针对性攻击，建议立即进行加固，处置建议见如下表格。

编号	业务地址	业务描述	风险	攻击检测	处置建议
1	17X.13.139.107:8104	107管理系统（存在弱口令漏洞）	高	暴力破解攻击	加强口令安全设置内网
2	17X.13.139.107:123	Telnet 远程管理	高		设置内网
3	17X.13.139.107:11555	SSH 远程登陆管理服务	高	暴力破解攻击	设置内网
4	17X.13.139.107:12345	SSH 远程登陆管理服务	高		设置内网
5	17X.13.139.107:12555	SSH 远程登陆管理服务	高		设置内网
6	17X.13.139.107:44444	SSH 远程登陆管理服务	高		设置内网

客户价值

系统上线72小时后，效果显著

116条
- 发现116条外网攻击，对暴露在外业务进行端口扫描

28例
- 自动下发28例黑名单，对境内外攻击进行阻断

1人
- 1人轻松保障X厂区安全可控

HUAWEI

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home and organization for a fully connected, intelligent world.

HUAWEI