SANGFOR
深信服科技

深信服智安全
SANGFOR SECURITY

融合安全、立体保护

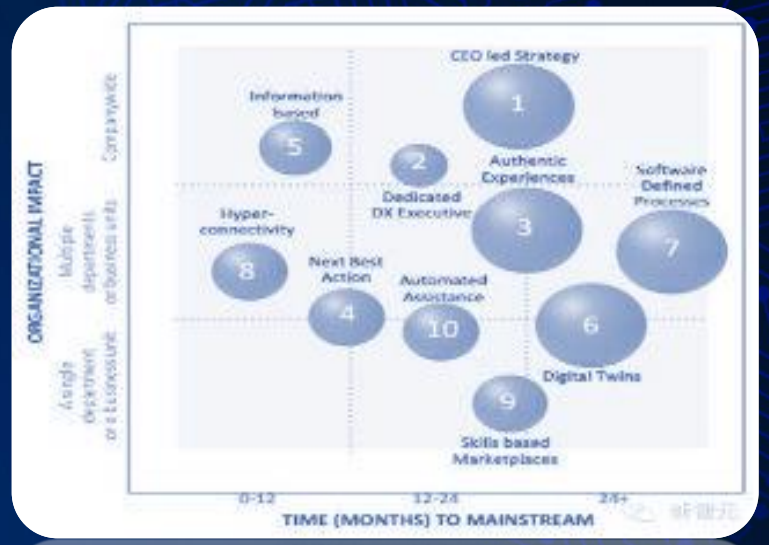
-有效构筑数字化转型道路的安全架构

数字化转型面临新的安全挑战

深信服智安全
SANGFOR SECURITY

业务层面

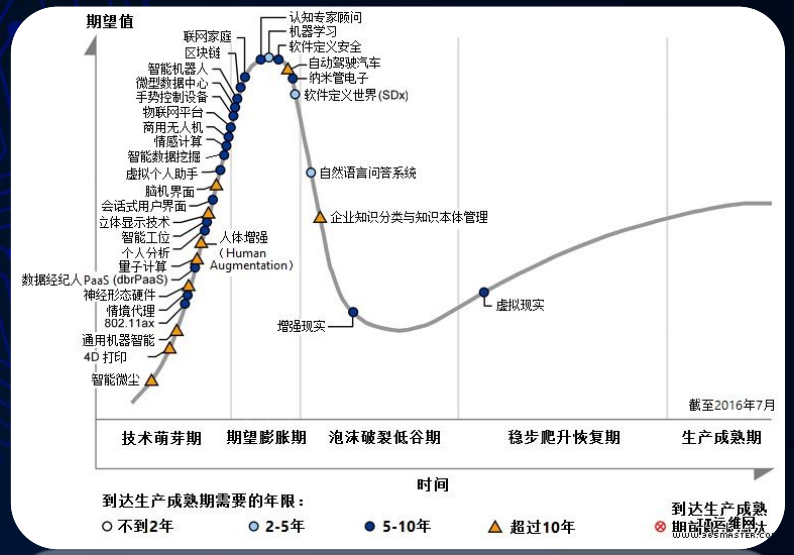
- 数字化转型导致暴露面快速增加。



2016年IDC数字化转型分析预测报告

技术层面

- 云计算、BYOD等新技术引入新风险。



Gartner发布2016年新兴科技技术成熟度曲线

外部威胁层面

- “黑灰产”威胁更加智能，攻防不对等。

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

2017年 OWASP TOP 10

传统安全体系正在失效


社工攻击
UEBA
ODAY攻击
勒索软件
人工智能
伊朗核电事件
租户安全
合作方攻击
斯诺登
APT
云安全
SWIFT被黑
Ddos
Tor
OPENSSL
鱼叉攻击
棱镜门
深度学习
漏洞攻击
数据泄密
EDR
暗网
美国大选邮件门
WikiLeaks
孟加拉央行8100万
GB/T 22239
Mirai
SaaS
虚拟化安全
bitcoin
方程式
毒液漏洞
黑产出售
雅虎10亿用户泄露
Target信息泄露

深信服智安全
SANGFOR SECURITY

我们长期依仗的安全技术手段为什么会失效？

“WannaCry” 事件反思

深信服智安全
SANGFOR SECURITY

为什么政府、运营商、医疗、能源等安全建设相对完善的行业也会受到大范围的影响？

事前

1、微软早在2017年4月份就发布了针对SMB漏洞的MS17-010补丁，更新率为什么那么低？

2、勒索软件时有发生，除了支付赎金就没有别的手段了吗？

事中

1、传统安全建设以防火墙、IPS、WAF等边界防护为主，边界一旦突破，防护还有效吗？

2、已知的漏洞都防护困难，如果是零日漏洞、新型变种病毒等未知威胁，还能防得住吗？

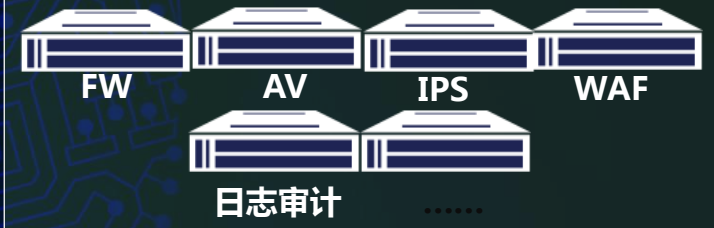
事后

1、如果我们无法绝对避免安全事件发生，能否在发生后第一时间发现？

2、我们有措施快速降低病毒扩算带来的损失吗？

传统信息安全建设弊端：防御为主

深信服智安全
SANGFOR SECURITY

事前	事中	事后
有哪些资产？ 有哪些漏洞？ 是否有策略？ 缺乏风险预知能力	 大量的安全建设投入以防御为主	是否有新漏洞？ 绕过能否检测？ 能否快速响应？ 缺乏及时发现及止损能力

“缺乏业务驱动”的“碎片化”安全建设

- 信息安全建设本质上是保证业务安全，而信息安全往往取决于业务保护的最薄弱环节。

图 APT Kill Chain攻击链条

安全架构过于复杂、难以落地

问题：面对如此复杂的安全架构，您需要多么强大的安全团队？

“亡羊补牢”还得能补得牢

深信服智安全
SANGFOR SECURITY

- 头痛医头的模式已经无法应对越来越复杂的安全形势
- 安全建设思路应该回归到降低业务风险的本质目标上来

有效的安全需要构建更容易落地的安全框架

深信服智安全
SANGFOR SECURITY

融合安全

- “事前、事中、事后”风险闭环管理

立体防护

- 基于全业务链的整体保护

简单有效

- 部署简单、灵活，产品易用

融合安全：“事前、事中、事后”风险闭环管理

深信服智安全
SANGFOR SECURITY

融合安全

1、在风险闭环管理的完整性方面，全面涵盖事“事前、事中、事后”；
2、基于产品功能、技术的融合，更好地识别安全风险，通过产品联动更高效解决问题。

事前：预知风险	事中：积极防御	事后：及时止损
自动化识别IT资产，实时扫描漏洞、风险，智能检查安全策略的有效性	L2-L7层防护，结合云端威胁情报的共享，多种设备联动防御	针对绕开边界进入内网的流量识别，进行失陷主机检测、云监测，联动响应

攻击者、事件的时间维度

立体保护：业务驱动安全建设的整体保护能力

深信服智安全
SANGFOR SECURITY

“空“：从外部视角，提供情报和外部联动能力。

“陆“：重构业务安全边界，防范外部入侵威胁。

“海“：持续检测与响应，形成内部业务自适应安全能力。

业务保护的空间维度

业务外部联动

外部威胁情报，云端沙箱与安全服务

业务边界安全

终端、网络接入安全，L2-L7层外部威胁防御，虚拟化/云环境的边界重构

业务承载环境安全

加强身份认证、加密与审计，通过持续监控与分析，逐步消除内部安全风险。

简单有效：安全建设更简单，更容易落地

深信服智安全
SANGFOR SECURITY

新架构需要新能力

深信服智安全
SANGFOR SECURITY

关键需求分析

融合安全
（事前、事中、事后风险闭环管理）

- 资产、漏洞及风险的可视能力。
- 风险、威胁及异常行为的动态感知能力。

立体保护
（海、陆、空全业务链整体防护）

- 全局安全可视，才能够看得清业务的整体安全性。
- 基于“防御、检测、响应”的闭环联动能力。

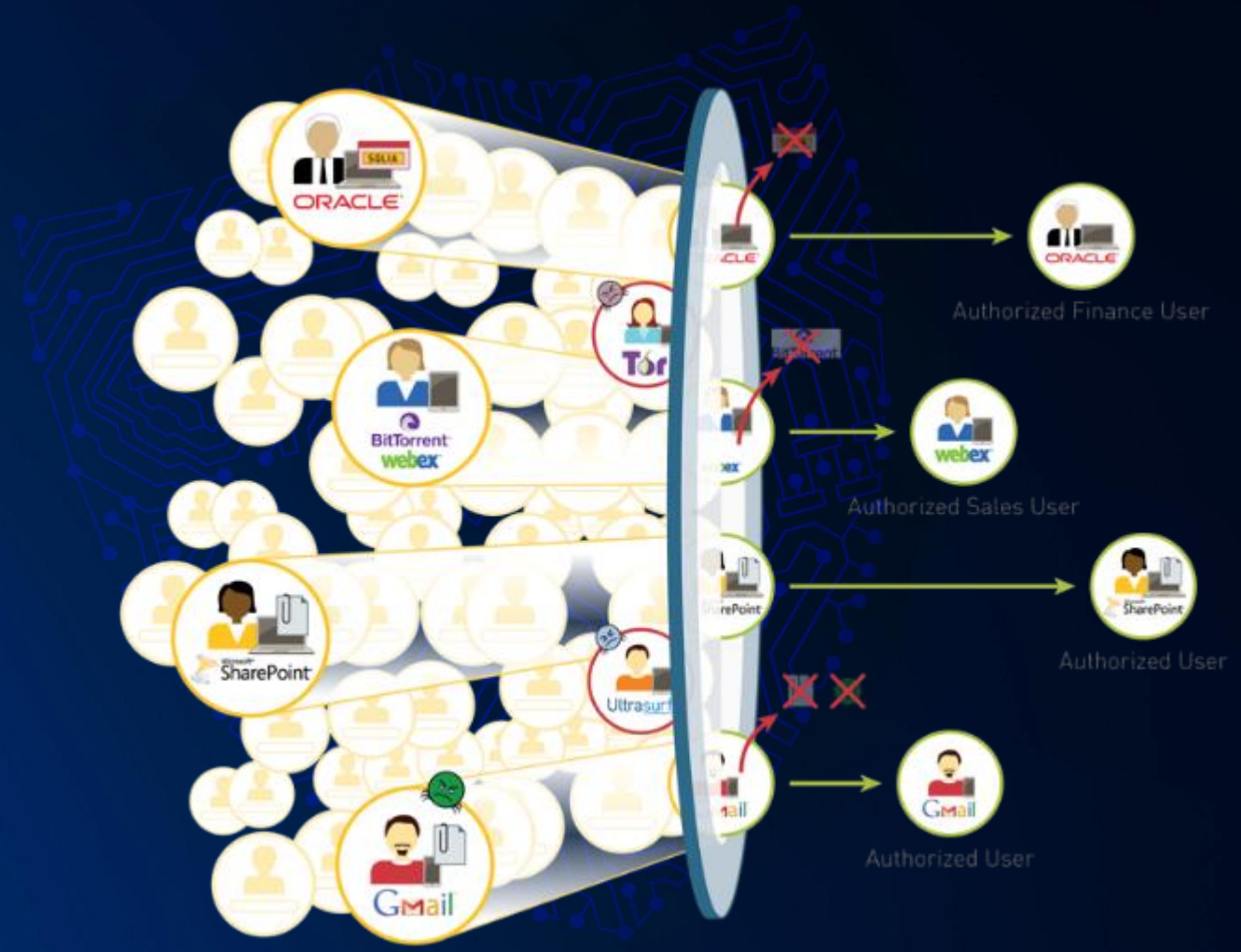
简单有效
（安全更简单、更容易落地）

- 安全可视是简单、有效的基础。
- 通过动态感知、闭环联动，才能有效处置风险。

应具备关键能力总结

1. 全网安全可视能力
2. 动态感知能力
3. 闭环联动能力

关键能力1：全网安全可视能力



口 资产状况和风险可视

- 对业务系统核心资产进行识别，如应用软件、用户、设备、内容等。
- 对业务资产存在的脆弱性和风险进行识别。

口 用户行为可视

- 分清业务的上下文关系，能随时甄别风险、应对威胁。
- 能够区分合法用户和非法用户，合法用户访问业务时是否在权限范围内。

全网安全可视能力展示界面

深信服智安全
SANGFOR SECURITY

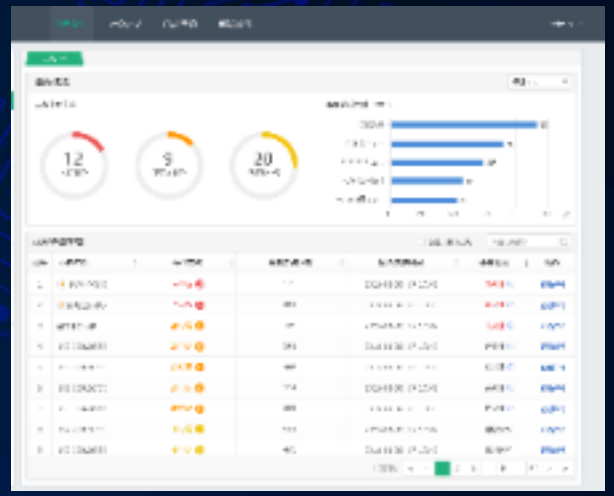
攻击防御大屏

全网安全态势大屏

非法外连大屏

新增风险资产发现

失陷业务/用户分析



危害取证分析

入侵事件处置

关键能力2：动态感知能力

深信服智安全
SANGFOR SECURITY

资产的新增或变更感知

- 通过业务识别引擎主动识别新增业务资产或变更新的业务资产。
- 发现资产变更后，自动对“变动资产”进行增量评估。减少新漏洞在网上暴露时间。

潜在的威胁及风险感知

- 实时汇集漏洞扫描信息，感知漏洞分别及危害情况；
- 对绕过边界防御的进入到内网的攻击进行检测，以弥补静态防御的不足。

安全事件感知

- 对内部重要业务资产已发生的安全事件进行持续检测，第一时间发现已发生的安全事件。

异常行为感知

- 对内部用户、业务资产的异常行为进行持续的检测，发现潜在风险以降低可能的损失。

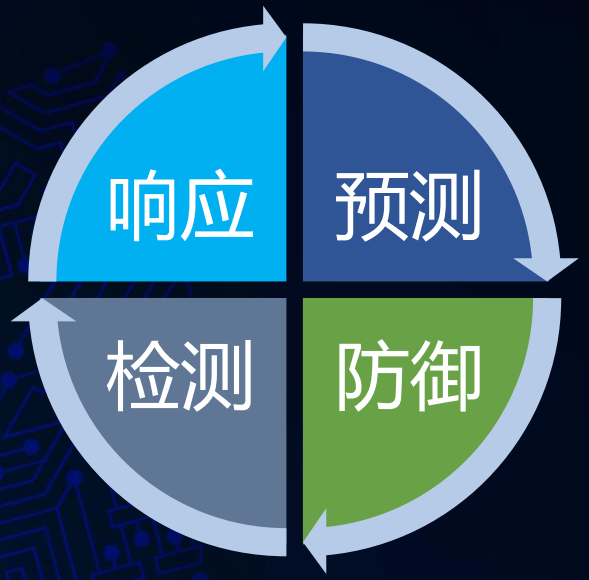
基于大数据的动态感知能力

通过持续检测，及时发现风险、事件

关键能力3：闭环联动能力

深信服智安全
SANGFOR SECURITY

闭环能力



- 防御、检测、响应和预测，形成闭环，应对各种攻击。
- 以智能集成联动的方式工作，应对高级威胁。

联动能力

云端联动

云端沙盒、网络安全监测云服务、威胁情报等，与内部业务及安全设备联动，增强对抗能力

平台与产品联动

平台与边界安全产品联动，下发拦截策略，提升攻击成本

产品内部联动

产品内部防御、检测、响应等模块智能联动，阻断攻击。

终端检测与响应联动

终端检测与响应EDR软件，快速定位威胁文件，阻断隔离

示例：下一代防火墙内部产品联动

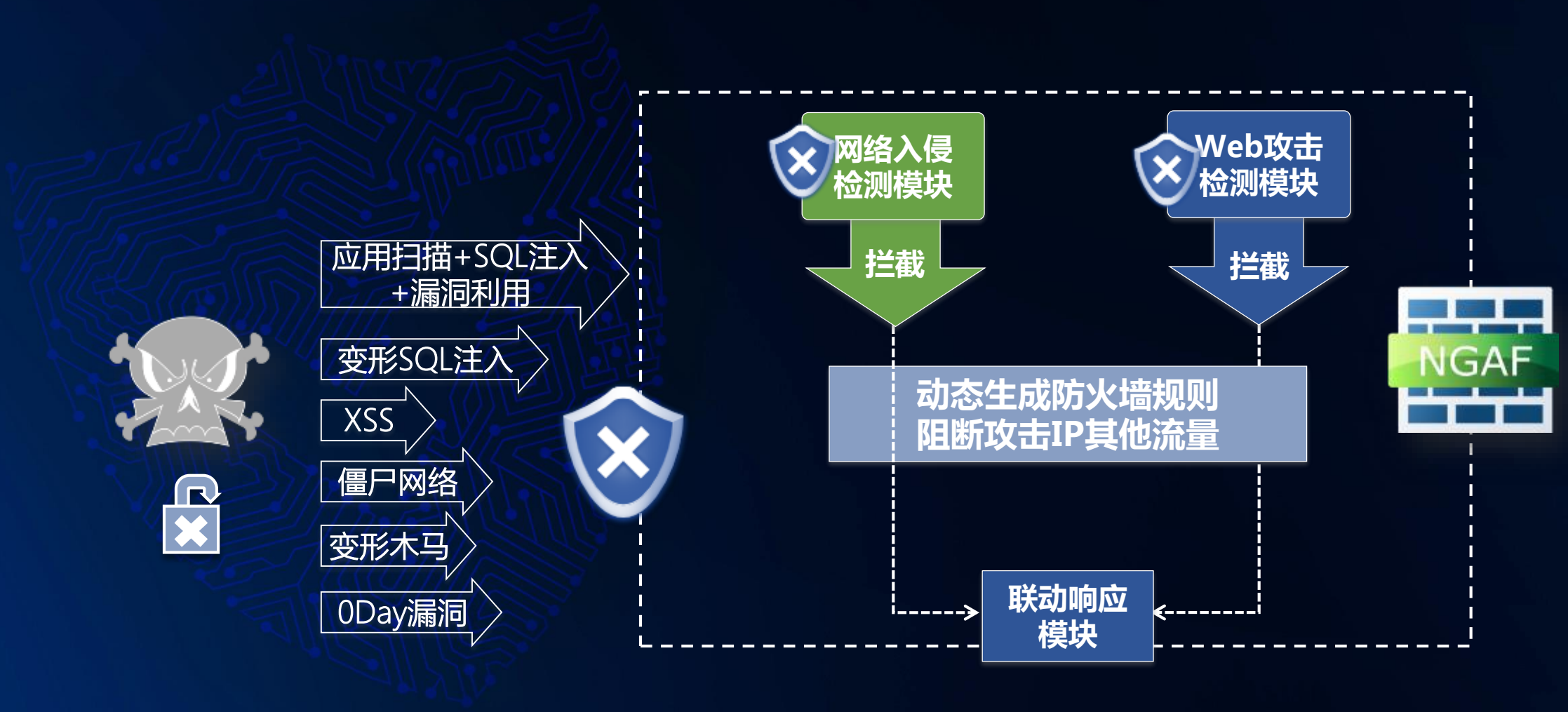
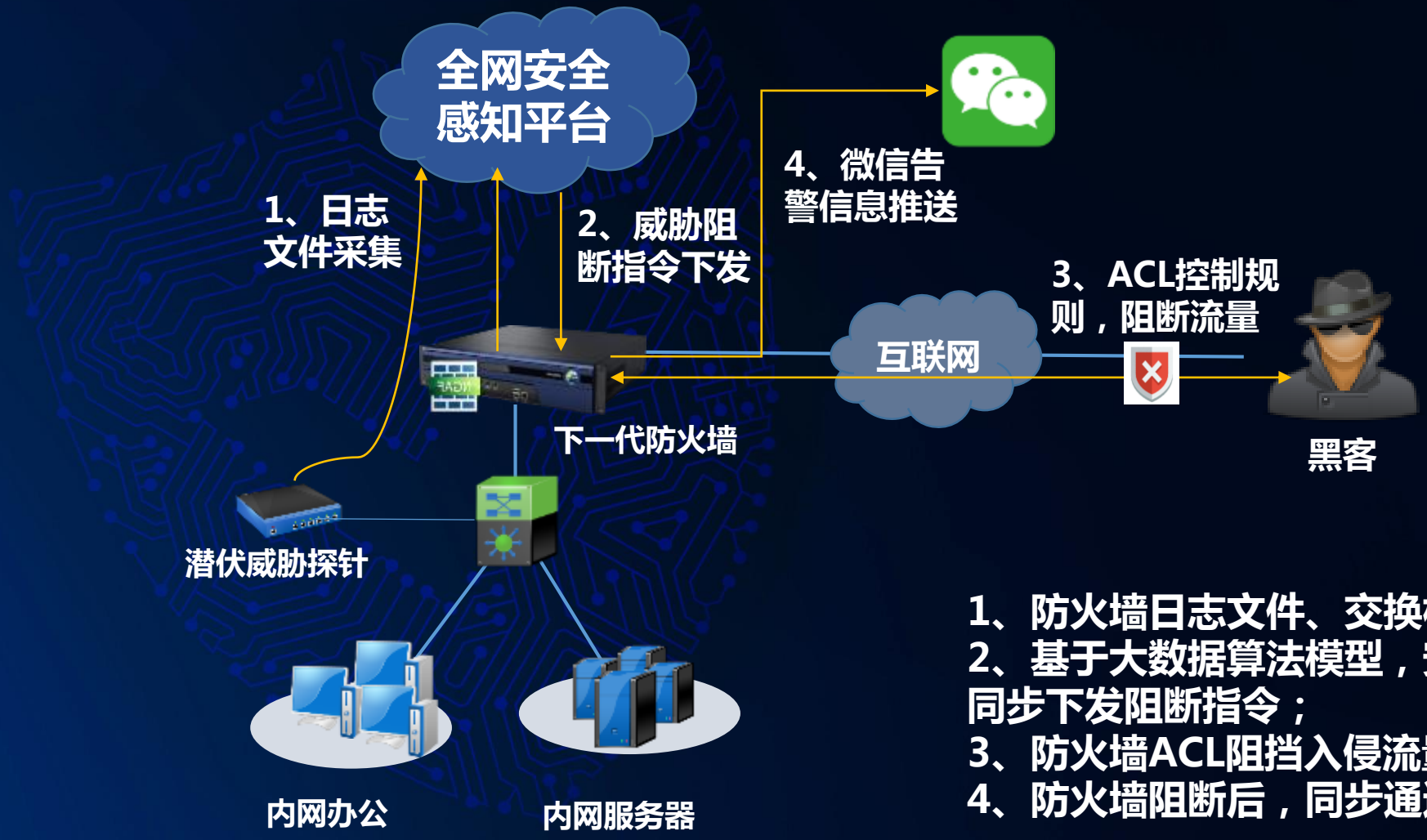


图 深信服下一代防火墙产品内部的模块联动

示例：安全感知平台与下一代防火墙联动



1、防火墙日志文件、交换机流量采集至安全感知平台；
2、基于大数据算法模型，安全感知平台发现威胁，并同步下发阻断指令；
3、防火墙ACL阻挡入侵流量。
4、防火墙阻断后，同步通过微信给用户发送告警信息。

示例：云端闭环联动


访问者
WEB访问
正常时期
风险监测服务
7*24小时监控网站异常
敏感时期
应急处置服务
云防御+安全专家值守
攻击对抗
监测\评估
Web网站
受护网站
受护业务
管理员
零部署
零维护
更放心

有效的安全需要构建更容易落地的安全框架

深信服智安全
SANGFOR SECURITY

融合安全

- “事前、事中、事后”风险闭环管理

立体防护

- 基于全业务链的整体保护

简单有效

- 部署简单、灵活，产品易用

深信服安全产品族谱

深信服智安全
SANGFOR SECURITY

云端服务：安全智能服务

威胁情报 | 风险评估 | 安全运营 | 应急响应 | 合作伙伴方案

EMM移动安全管理

SSL/IPSec VPN

上网行为管理

下一代防火墙

云安全NFV安全资源池

全网安全感知平台

WOC&MIG

终端检测与响应EPS

其他安全产品

不同场景下的信息安全解决方案

深信服智安全
SANGFOR SECURITY

移动办公环境（PC端、手机端）

EMM　SSL VPN　威胁探针

EC

外部用户接入环境

EC　EMM　SSL VPN

互联网/移动互联网

数据中心/私有云环境

安全边界区

NGAF

DMZ区

NGAF　威胁探针

内部、外部服务区

威胁探针

防御类服务　检测类服务　响应类服务　审记类服务

管理区

全网安全感知平台

SC集中管理平台

云安全资源池

VPC

局域网办公/园区网络环境

用户行为区

AC

终端安全管理及边界区

NGAF　威胁探针

终端接入区

广域网/分支互联环境

MIG　WOC

广域网/内部专网

WOC　MIG

公有云/行业云/混合云环境

租户安全

防御类服务　检测类服务　响应类服务　审记类服务

安全资源池

平台安全

平台安全组件

整体安全框架建设步骤建议

深信服智安全
SANGFOR SECURITY

STEP 01

构建关键边界安全

通过融合的边界安全产品，构建您关键业务的安全“护城墙”；

STEP 02

更广泛的安全边界+安全感知平台

更多节点需要部署AF，延伸安全的保护范围；并构架感知平台，为客户统一呈现安全态势；

STEP 03

安全加固与持续深化

建议重要业务系统安全加固，重要门户购买安全监测服务；

STEP 04

全网安全可视、动态感知

核心节点部署探针收集东西向流量或不经过AF的流量统一到感知平台

STEP 05

持续的安全服务

整个安全架构需要用好，则通过持续购买安全即服务获取。

SANGFOR SECURITY
深信服智安全

做实用的安全，
让每个组织的安全建设更有效、更简单

深信服智安全
SANGFOR SECURITY