



2020 北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

内生安全 从安全框架开始

ENDOGENOUS SECURITY:
STARTING FROM A CYBERSECURITY FRAMEWORK

一个工作组

一套紧密协同机制

规划方法、工具集、模型、架构和项目纲要

内生安全的关键是管理

内生安全

自主

自主

自成长

自成长

自适应

自适应

漏洞是不可避免的

超过 **85%** 的安全威胁来自于 **内部**

所有的体系都是人来操控管理的

不管技术多高
我们的体系还是会失效



2016年美国东海岸断网

缺乏有效管理



2017年“永恒之蓝”事件

缺乏有效管理



2020年推特账号被劫持

缺乏有效管理

新管理模式

由数据驱动，实现对各方面要素的有效管理

发现和规避攻击，克服人的不可靠性、弥补人的能力不足

内生安全 → 新形态的网络安全管理模式

管理的关键是**框架**

系统工程

涌现

$1+1>2$

内生安全也具有“涌现”效应

能够实现“ $1+1>2$ ”的效果

建设内生安全，采用的是系统工程的思想

“局部整改”为主的安全建设模式

体系化缺失 碎片化严重 协同能力差

内生安全框架

将安全需求分步实施落实，逐步建成面向未来的安全体系

支撑各行业的建设模式从“局部整改外挂式”走向“深度融合体系化”

内生安全框架的 **3** 个重点

“理清楚”

“建起来”

“跑得赢”

“理清楚”



体系化地梳理、设计出所需的安全能力



梳理时充分考虑所有可能涉及到的问题



设计时根据实际情况挑选、组合和规划

“建起来”



融合是建设的关键，做到深度融合、全面覆盖



安全能力组件化，将安全能力合理地分配部署



具体建设过程中，需要全景化的技术部署模型

“跑得赢”



缺乏安全运行的安全系统，相当于“靠天吃饭”



把管理作为关键，就能跑赢漏洞、内鬼、黑客



确保安全运行的可持续性，实现安全管理闭环

框架的关键是组件化

信息化系统的替代是“立新破旧”的过程

对老系统用老办法，新系统用新办法，会造成巨大浪费

“统一设计，分步实施” 把安全框架组件化

让组件既是新体系的一部分，又能部署到老系统中

组件与信息化体系化地聚合

是安全框架落地的关键

“十大工程 五大任务”

内生安全框架的具体落地手册

某“新基建”项目

136个信息化组件 29个安全区域场景 79类安全组件



2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE
全球网络安全 倾听北京声音



北京2022年冬奥会官方赞助商
Official Sponsor of the Beijing Winter Olympic Games 2022



2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE
全球网络安全 倾听北京声音

从安全框架开始

推动网络安全产业再上新台阶！