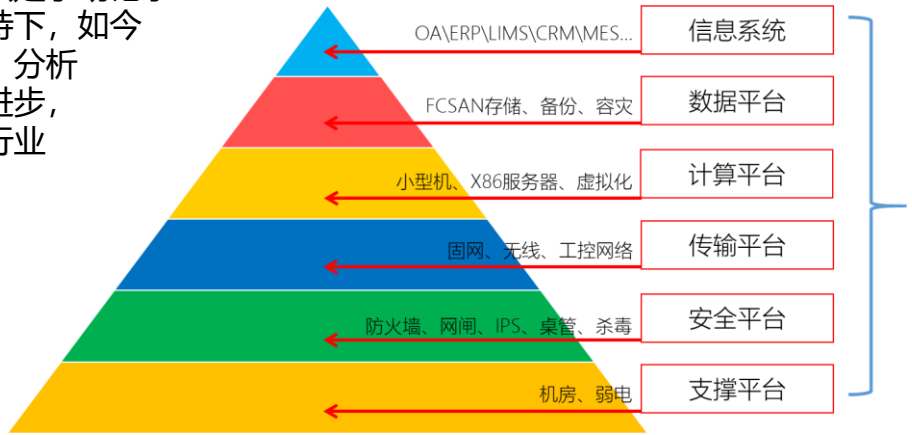

Hillstone
山 石 网 科
方案名称：集团公司网络安全解决方案
个人信息：杨飞-太原市远征科贸有限公司

行业信息化构成

随着信息化在药企中不断的成熟和深入应用，在药品研发、生产制造和销售过程中，企业对管理和经营都依赖于信息化平台，各种内部系统如**OA**、**ERP**、**LIMS(**实验室信息管理系统**)**、生产管理系统、质量管理系统、**CRM**系统等。

在经过数字化建设后，我们数据中心的规模不仅增加，系统多了，数据量也变得更加庞大，各方面产生的风险也随之大幅增加。网络安全不仅仅是软件的安全，一系列与网络、与计算机相关的一类的安全都是要考虑的。比如服务器、环境的安全，作为制造业还要考虑生产线、质量管理系统的安全。

在“互联网+”浪潮的席卷下，医药行业的信息化建设也开始驶入快车道。事实上，医药行业是一个最需要进行信息化建设和改造的行业，以药物临床试验为例，需要大样本量、高精细度的数据提供支持。传统方法是手动记录数据、纸质文件存档数据，而在信息化技术和互联网技术的加持下，如今已有不少医药企业开始采用信息化的方式进行数据采集、处理、分析及存储，这极大地提高了医药企业的研发和运营效率。技术的进步，带来了效率的提升，却也埋下了数据安全的隐患。尤其是其他行业不时爆出的信息泄露事件，向医药行业敲响了信息安全的警钟。



企业面临的威胁

内部威胁日益增长

- 内部管理制度有待完善
- 内部人员监管有待加强

数据安全保障困难

- 业务场景复杂，监管场景高度定制
- 数据种类多，数量大，监管覆盖难
- 参与方众多，人员账号关系复杂

数据滥用无法识别

- 数据运维人员权限大，难以分辨对敏感数据的访问是工作需要还是个人行为。

外部形势愈发严峻

- 医药行业数据价值大，黑客觊觎
- 第三方机构数据交换，可能导致数据泄露

需求分析

网络边界风险

- 外部攻击
- 移动互联
- 端口开放
- 钓鱼邮件

终端安全风险

- 系统漏洞
- 病毒木马
- 系统弱口令
- 移动存储介质

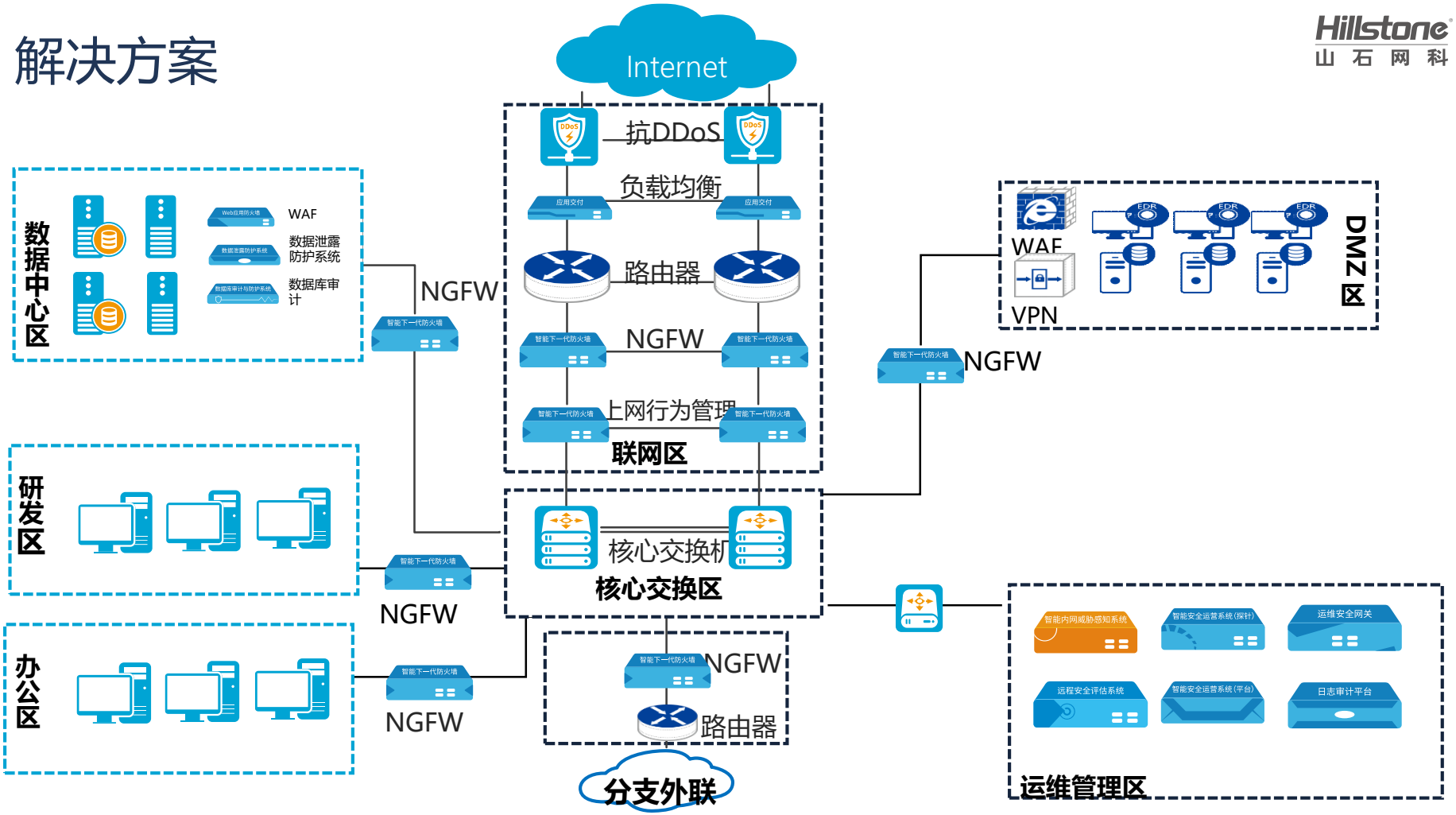
应用系统风险

- 业务系统漏洞
- 访问控制不严
- 商业竞争
- 数据安全问题

信任风险

- 第三方运维人员
- 身份认证不全
- 运维操作不知
- 恶意操作无控
- 安全意识薄弱

解决方案


Internet
抗DDoS
负载均衡
路由器
NGFW
上网行为管理
联网区
数据中心区
WAF
数据泄露防护系统
数据库审计
NGFW
DMZ区
WAF
VPN
NGFW
研发区
核心交换机
核心交换区
NGFW
办公区
NGFW
NGFW
路由器
分支外联
智能内网威胁感知系统
智能安全运营系统(探针)
运维安全网关
远程安全评估系统
智能安全运营系统(平台)
日志审计平台
运维管理区

方案优势

构建三维一体全方位数据防护

- 从数据库服务器的底层系统、网络、数据库三个层面分别进行三位一体的立体防护。从根本上保证数据库服务器的底层操作系统免受攻击、网络层面实现有效的网络防护、数据库层面实现合规访问控制和攻击防护，彻底解决数据库的安全防护难题。

提升体系化纵深联动防御

- 通过大数据分析技术发现潜在的入侵和高隐蔽性攻击，预测即将发生的安全事件并与安全防护设备形成联动能力，自动安全调整访问控制策略下发至防御设备，第一时间阻断(通过联动防御设备进行安全阻断，如WAF、IPS、防火墙等）攻击者的连接，形成安全闭环，提升集团信息安全风险管理和应对能力。

Thanks

Hillstone
山石网科

为您的安全竭尽全力！

400-828-6655

https://www.hillstonenet.com.cn