

高效运维 智创未来

IT 运维升级之路与实践分享

汇报人：范楷

卓豪（中国）技术有限公司

关于卓豪 (ZOH0)

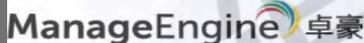
• 专注于企业级软件研发创新技术公司

- 成立于1996年。全球拥有18000名员工，其中80%为开发人员
- 2002年在北京成立中国区总部，拥有200多名员工，在上海、广州、深圳、南京、杭州、福州、济南、成都、武汉、郑州、西安、沈阳等地设有分支机构。



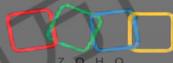
1996

电信级
物联网管理平台



2002

企业IT运维
管理解决方案



2004

企业合作及
生产性应用

ManageEngine 提供企业级 IT运维管理解决方案

综合网络管理

- 综合网络性能监控
- 应用性能管理
- 网络配置自动化管理
- 网络流量分析
- IP地址和交换机端口管理



IT服务管理

- IT服务台
- 全生命周期IT资产管理
- CMDB可视化 & ITIL流程
- 客户支持系统



IT安全管理

- 系统及应用日志分析
- 防火墙日志分析
- 漏洞分析
- 特权账户管理



终端管理

- 桌面及移动终端管理
- MDM & BYOD管理
- OS自动化部署
- 远程支持
- 终端用户体验



身份及访问管理

- 微软AD自动化管理
- Exchange审计
- 用户自助服务门户
- Microsoft 365管理



IT数据分析

- 数据多维度可视化
- 自定义数据分析操控版



ManageEngine 卓豪

ManageEngine客户

20万+

ManageEngine拥有全球20万客户。而且客户的数量还在不断地增加，特别是来自中国区的客户越来越多。

200

ManageEngine为全球不同语言国家提供IT运维解决方案。200多个国家地区的企业都在使用卓豪的产品。

70%

在500强企业中，有超过70%企业的IT运维管理已经依托于ManageEngine产品线。



分享主题：

一、企业信息化运维本质探讨

二、运维升级之路实践案例分享

三、基于AI驱动下的IT运维管理体系

企业网DINet
2025全国甲方IT选型规划大会

企业网DINet
2025全国甲方IT选型规划大会

企业网DINet
2025全国甲方IT选型规划大会

企业信息化运维

本质探讨

IT 运维 百家争鸣

ITIL

项目管理

持续交付

XOps

ITSM

自动化运维

敏捷开发

敏态

稳态

DevOps

全链路监控

APM

无缝集成

业务服务管理

DLP

AIOps

CMDB

可观测性

简化IT管理

IT 运维如履薄冰



为**业务**持续提供优质服务是运维的目标



企业网DINet

2025全国甲方IT选型规划大会

企业网DINet

2025全国甲方IT选型规划大会

企业网DINet

2025全国甲方IT选型规划大会

企业信息化运维

案例分享

难题与困境

“三高”困境



管理层

- ? 业务连续性如何保障
- ? 运维成本如何控制
- ? 安全合规高压
- ? 部门价值如何体现
- ?

“三难”困境



执行层

- ? 救火式工作
- ? 故障排查困难
- ? 沟通成本高
- ? 技能提升困难
- ?

“三不”困境



业务层

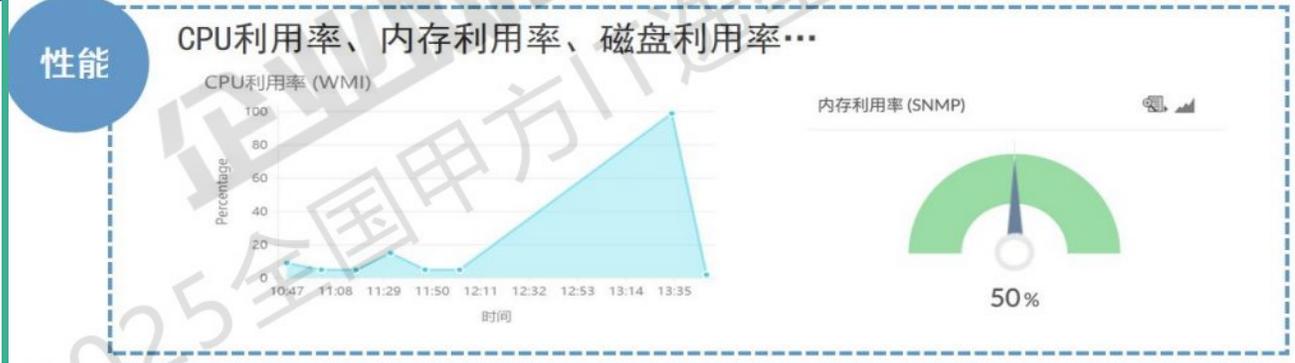
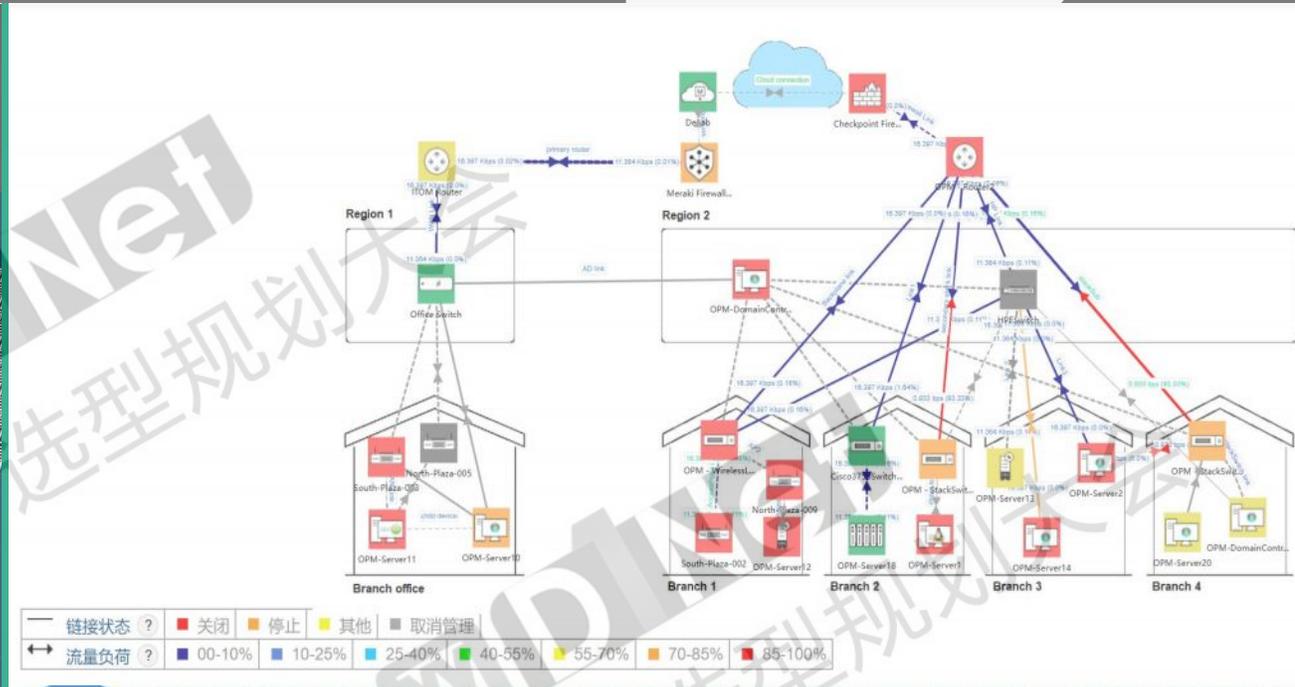
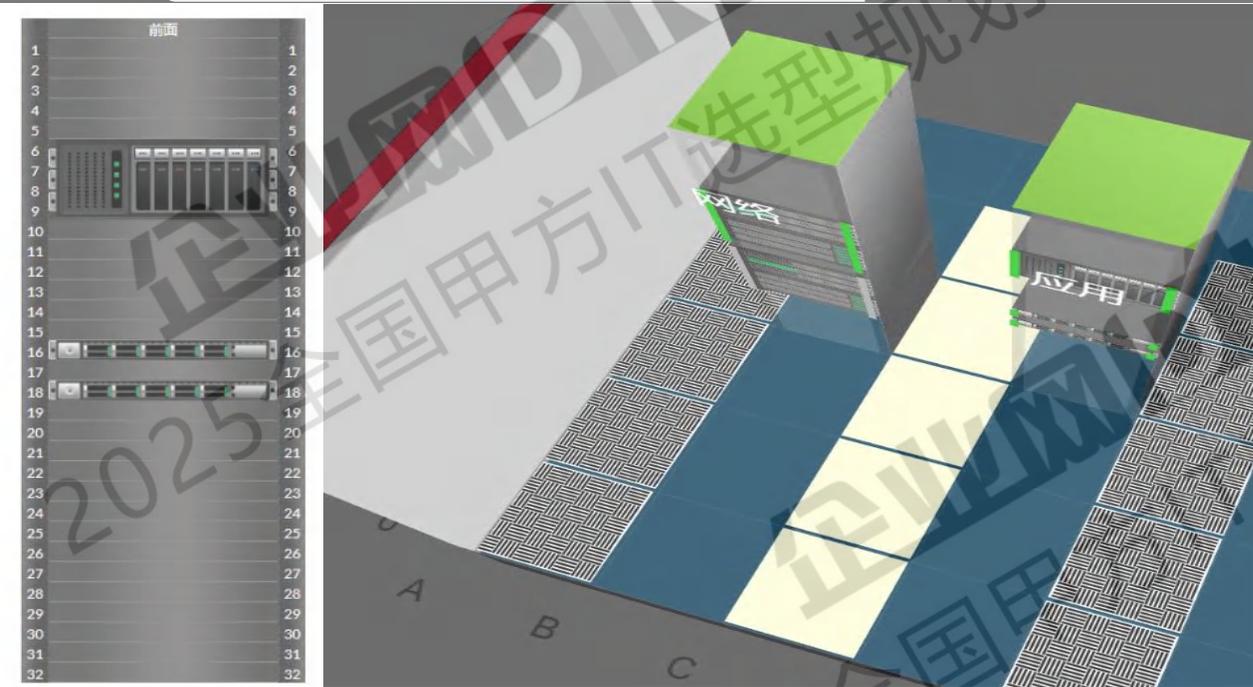
- ? IT总是姗姗来迟
- ? 系统为何慢卡顿
- ? 故障处理到哪个阶段
- ? 新系统该如何使用
- ?



数据中心-资源健康状态监控

数据中心3D可视化

动态实时拓扑



可用性监控

智能洞察-AI故障预测

自适应阈值



启用自适应阈值

通过使用机器学习学习数据模式来自动配置动态阈值。

监视器	动作
CPU使用率	<input checked="" type="checkbox"/>
内存使用率	<input checked="" type="checkbox"/>
响应时间	<input checked="" type="checkbox"/>

小时	预测	注意	有故障的	危急的
0:00-1:00	34	39	42	49
1:00-2:00	36	41	44	51
2:00-3:00	44	49	52	59
3:00-4:00	58	63	66	73
4:00-5:00	54	59	62	69

AI预测报表

机器学习

增长趋势预测



利用率预测

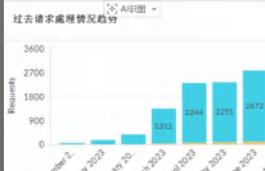


监视器 > 内存利用率 (SNMP) > 预测 - [28/06/2024 00:00 - 05/07/2024 01:00]



管理成果

全局



故障分析 日报、周报

周次	分析內容	日期	文件夾
01周	数据分析	2023/5/19 10:28	文件夾
02周	数据分析	2023/5/19 10:28	文件夾
03周	数据分析	2023/5/19 10:28	文件夾
04周	数据分析	2023/5/19 10:29	文件夾
05周	数据分析	2023/5/19 10:29	文件夾
06周	数据分析	2023/5/19 10:29	文件夾
07周	数据分析	2023/5/19 10:28	文件夾
08周	数据分析	2023/5/19 10:28	文件夾
09周	数据分析	2023/5/19 10:29	文件夾
10周	数据分析	2023/5/19 10:29	文件夾
11周	数据分析	2023/5/19 10:29	文件夾
12周	数据分析	2023/5/19 10:29	文件夾
13周	数据分析	2023/5/19 10:29	文件夾
14周	数据分析	2023/5/19 10:29	文件夾
15周	数据分析	2023/5/19 10:29	文件夾
16周	数据分析	2023/5/19 10:29	文件夾
17周	数据分析	2023/5/19 10:29	文件夾
18周	数据分析	2023/5/19 10:29	文件夾
19周	数据分析	2023/5/19 10:29	文件夾
20周	数据分析	2023/5/19 10:29	文件夾
21周	数据分析	2023/5/19 10:29	文件夾
22周	数据分析	2023/5/19 10:29	文件夾

CIO

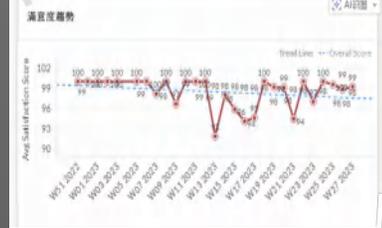


- 01-桌面終端服務 (故障請求) .xlsx
- 02-非生產集采平台 (SRM) 服務 (故障請求) .xlsx
- 03-ERP系統服務 (故障請求) .xlsx
- 04-PLM系統服務 (故障請求) .xlsx
- 05-桌面雲服務 (故障請求) .xlsx
- 06-AD域管理服務 (故障請求) .xlsx
- 07-BPS系統服務 (故障請求) .xlsx
- 08-供應商關係管理系統 (SRM) 服務 (故障請求) .xlsx
- 09-ITSM系統服務 (故障請求) .xlsx
- 10-網路平台服務 (故障請求) .xlsx
- 周TOP10分析 (03-18) .xlsx

變更經理



用戶滿意度



滿意度調查表記錄

Response Resolved	User	Survey Name	Associated Request	Question Text	Type	Answer
No Value	No Value	新件-熱管 備用度調查	No Value	滿意度調查	Open Scale	1 out of 5
2023/2/23	Magge Y.Y. (何怡君)	新件-熱管 備用度調查	新件-熱管 備用度調查	滿意度調查	Open Scale	3 out of 5
						5 out of 5
						5 out of 5

安全防控

守护核心资产安全与合规

精细化权限管理



特权账号/密码及其访问控制管理。基于角色的访问控制，防止权限越权和信息泄露，保障数据访问安全。

审计与日志溯源



分析关键操作与变更日志，通过多种合规标准的导出与审计，便于追溯。

数据加密分级保护



字段级数据加密，自定义安全级别设置，有效保护敏感数据。

身份验证强化机制



多因素认证（MFA），集成LDAP/AD，统一账户管理，提升身份验证安全性。

漏洞管理和合规检查



对操作系统和应用的风险和漏洞进行全面扫描、持续监测、严格评估，和完整修复。

管理成果



儀表板 訪問審核 訪問分析 告警 配置

匯總報告

文件名

經常訪問的文件	C:\Users\Administrator\AppData\Roaming\FortClient\logs\trace\certificates.txt
經常修改的文件	C:\Users\Administrator\AppData\Roaming\FortClient\logs\trace\FortTray_1.log
最近訪問的進程	C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\CachedImage_1080_1920_PC
最近訪問的用戶	C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\CachedImage_1080_1920_PC
N天內訪問的文件	C:\Users\Administrator\AppData\Roaming\FortClient\logs\trace\gimessenger_1.log
N天內修改的文件	C:\Users\Administrator\AppData\Roaming\FortClient\logs\trace\issvnpib_1.log

基于用户的报表

用户报表-所有事件

用户报表成功事件

用户报表失败事件

基于主机的报表

主机报表-所有事件

主机报表成功事件

主机报表失败事件

基于共享的报表

共享报表-所有事件

共享报表成功事件

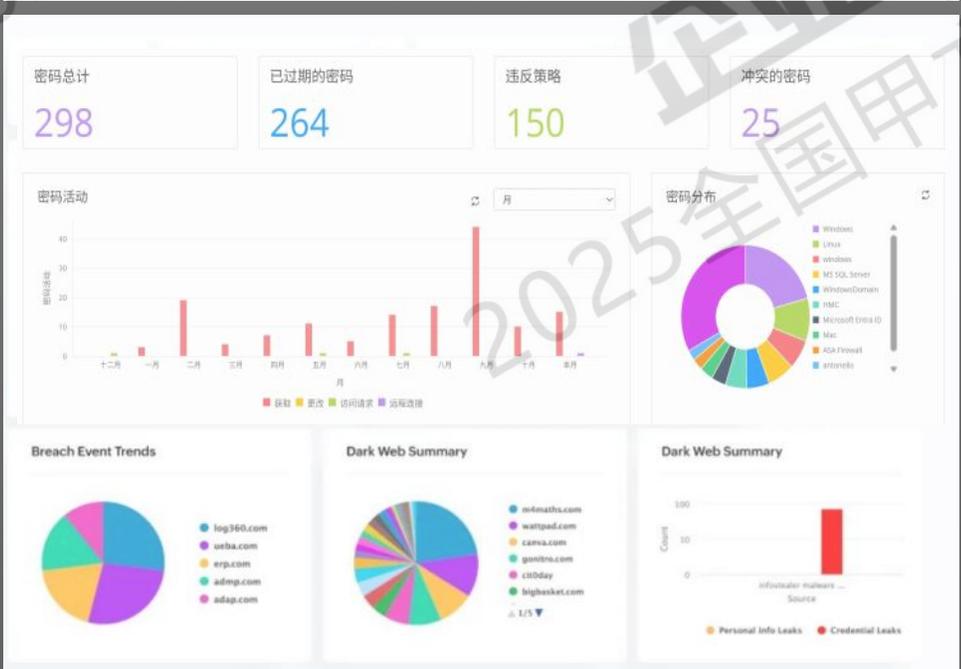
共享报表失败事件

基于位置的报表

位置报表-所有活动

位置报表-成功事件

位置报表-失败事件



自动化运维

自动化派单

#443 监控告警-OA数据库服务器_进程postgres.exe已停止
告警平台 时间 2025-03-10 16:08:06 | 逾期: 2025-03-10 16:38:06 (延迟 252 天)

告警自动生成工单

自动生成工单
工单自动分配
基于AI原因分析

告警通知

AI ZIA Boot 2025-03-10 16:08:06

AI推荐处理建议:
1. 检查进程服务状态登录到设备 OA数据库服务器 (IP: 192.168.0.16).
通过命令行执行以下命令检查进程服务状态: Get-Service | Where-Object { \$_.Name -like "*postgres*"} 或者通过Windows服务管理器查看进程服务是否已停止.
2. 尝试重启进程服务如果服务已停止, 尝试重新启动该服务: 打开服务管理器 (services.msc), 找到进程服务, 右键点击, 选择 启动, 或者使用命令行启动: Start-Service

自动化通知

监控告警通知群 16:50 17:27

OPM监控通知 BOT

OPM告警通知:
告警来源: 192.168.0.26
告警严重性: 严重
告警信息: 内存利用率为48%, 此监视器的阈值为40%: Top 3 Processes:-java.exe - 7.1379
4.083%:java.exe - 3.541%

OPM监控通知 BOT

OPM告警通知:
告警来源: 192.168.0.26
告警严重性: 问题
告警信息: C:的设备分区信息(%)为40 百分比, 此监视器的阈值为35 百分比

OPM监控通知 BOT

OPM告警通知:
告警来源: 192.168.0.26
告警严重性: 问题
告警信息: 磁盘利用率为40%, 此监视器的阈值为35%

分级发送告警

告警自愈

【监控告警请关注】OA数据库服务器 (192.168.0.16) 进程 postgres.exe 已停止, 时间: 2025-03-14 03:38:05.

返回结果

执行工作流 工作流执行成功

工作流名称: Windows_PostgreSQL进程自动恢复

触发告警: [严重] OA数据库服务器 - 进程postgres.exe已停止

执行时间: 2025-03-14T03:38:10 (告警产生后5秒)

步骤序号	步骤名称	执行结果	详细信息
1	工作流触发	成功	已成功捕获来自设备 OA数据库服务器 (IP: 192.168.0.16) 的告警信息。告警ID: INC-20250314-03805。
2	通过WMI连接服务器	成功	已使用服务账户成功建立与 192.168.0.16 的连接。
3	检查进程状态	成功	确认 postgres.exe 进程不存在, 与告警信息一致。
4	尝试启动服务	成功	已执行命令启动服务 postgresql-x64-12, 服务状态返回为 Running。
5	服务健康检查	成功	等待10秒后, 成功连接到数据库 postgres 并执行 SELECT 1; 查询, 响应正常。
6	清除告警	成功	已向Opmanager告警管理器发送指令, 成功清除告警ID INC-20250314-03805。
7	关闭故障工单	成功	已关联到告警对应的工单ID WO-INC-20250314-03805, 并将其状态更新为“已解决”, 备注: “已通过自动化工作流完成进程恢复”。
8	发送执行摘要	成功	已向通知组 DB-Admins发送邮件通知。标题: “【自动化修复成功】OA数据库服务器PostgreSQL服务已恢复”。

执行流程
故障修复
告警解除
关闭关联工单

告警解除

自动化治愈

配置命令下发

执行Windows脚本

名称: 执行Windows脚本

本地服务器

目的设备: ?

命令行变量: --选择变量--

命令: cscript //Nologo %FileName%.vbs

脚本内容变量

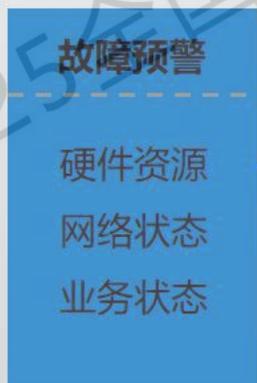
脚本内容: Start-Sleep -Seconds 10 # 检查启动状态 \$service.Refresh() if (\$service.Status - 'Running'){ Write-Log "PostgreSQL服务重启成功"

配置下发
脚本执行

运维升级之路总结

统一可见性

确保现有业务有序，稳定运行



智能洞察

主动防护，建立安全的IT环境



自动化驱动

将重复性的、标准化的操作自动化



运维对象

• 由黑盒到白盒

运维机制

• 由被动向主动

运维组织

• 由成本中心向价值中心

一体化运维平台

监控平台ITOM

流程平台ITSM

桌管平台UEM

安全分析平台SIEM

低代码平台

数据分析平台

数字化运维体系的演进在一体化底座上

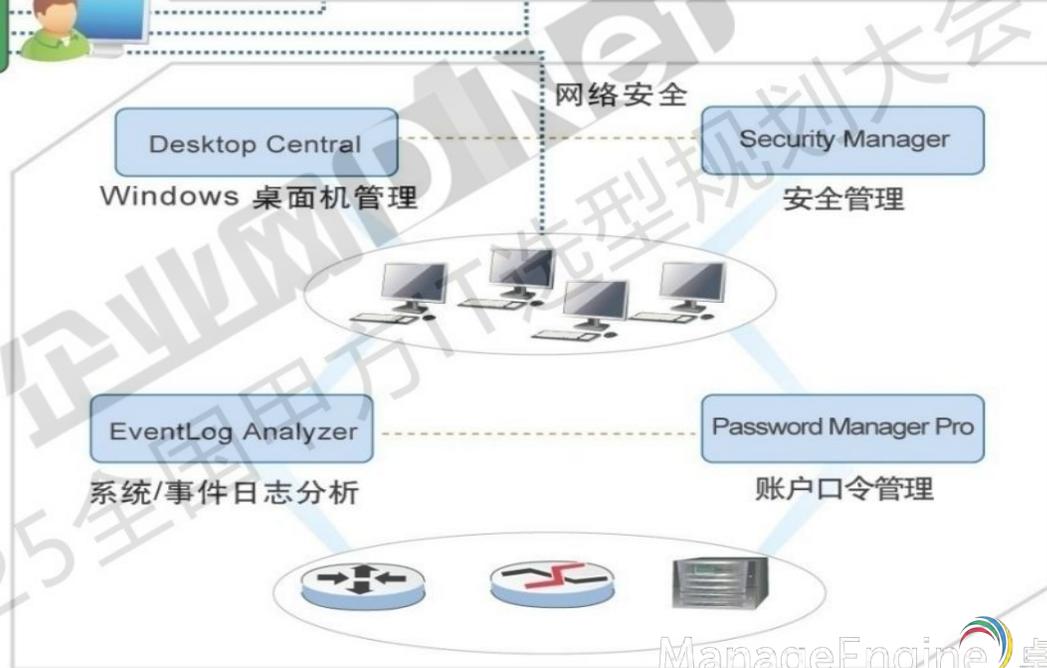
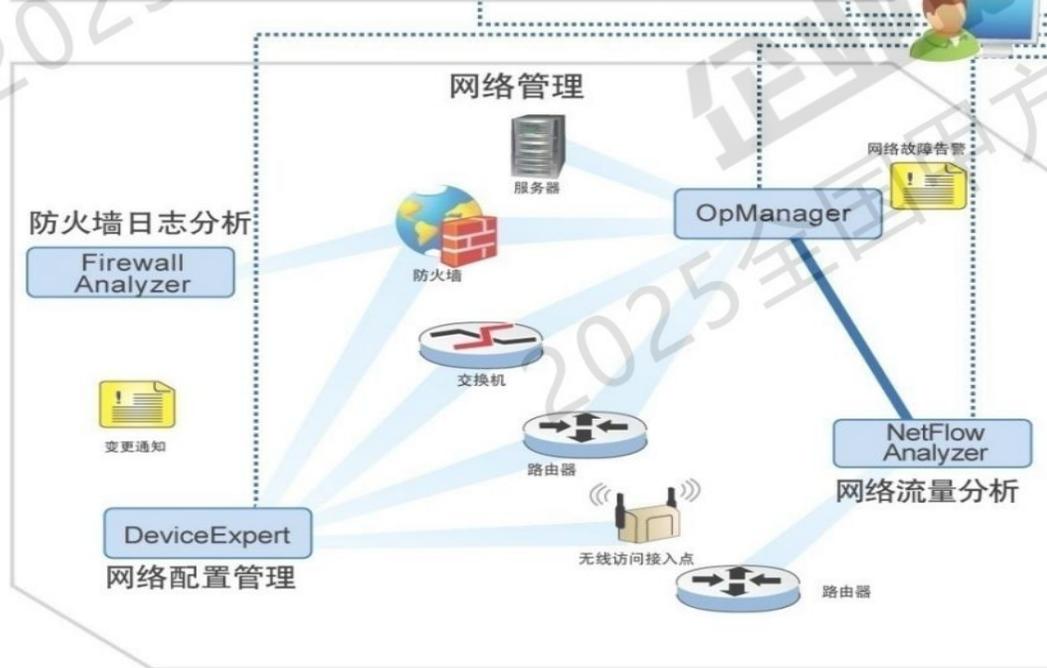
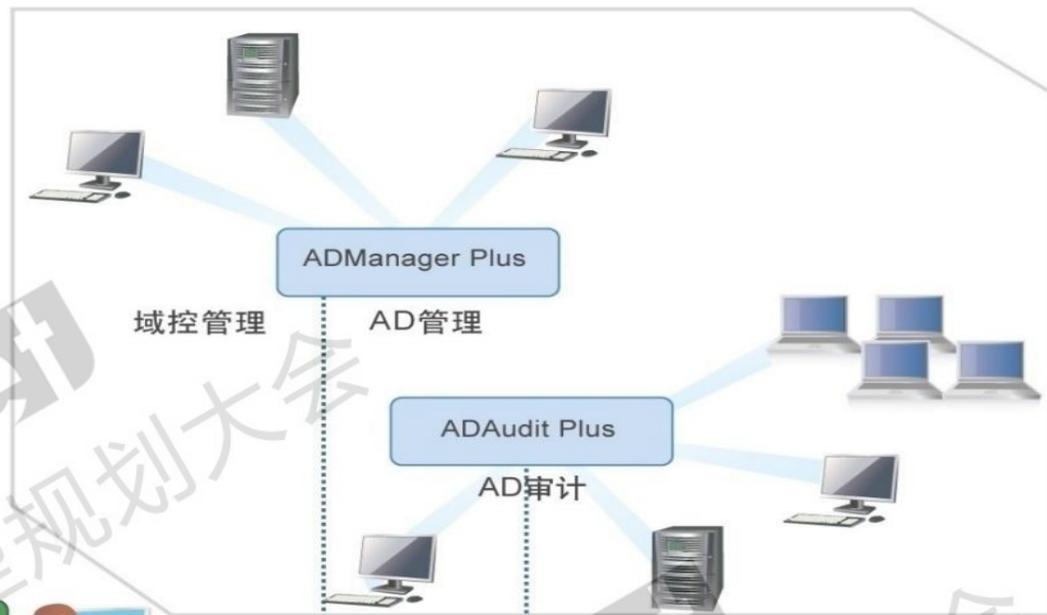
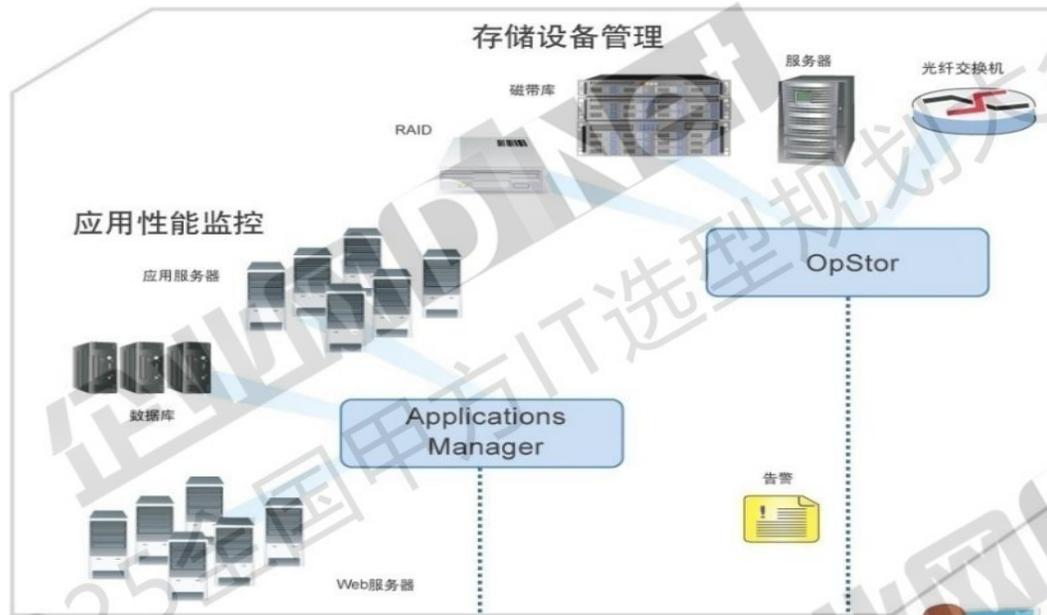
企业网DINet
2025全国甲方IT选型规划大会

企业网DINet
2025全国甲方IT选型规划大会

企业网DINet
2025全国甲方IT选型规划大会

AI驱动下的

全栈IT运维体系



以AI为驱动的运维体系



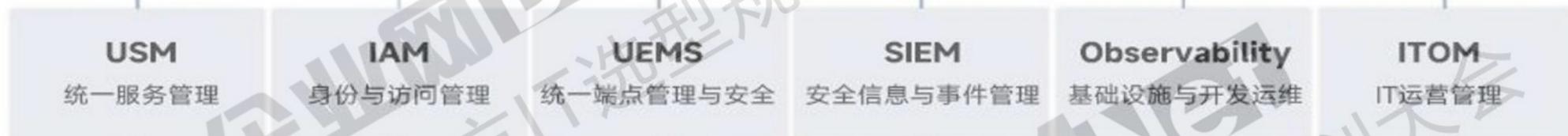
成果

受益方：高级管理人员、首席信息官(CIO)、首席信息安全官(CISO)

事件响应、业务连续性、灾难恢复、安全态势
员工体验、网络弹性、零信任、混合办公、治理风险合规 (GRC)

策略

受益方：IT项目经理

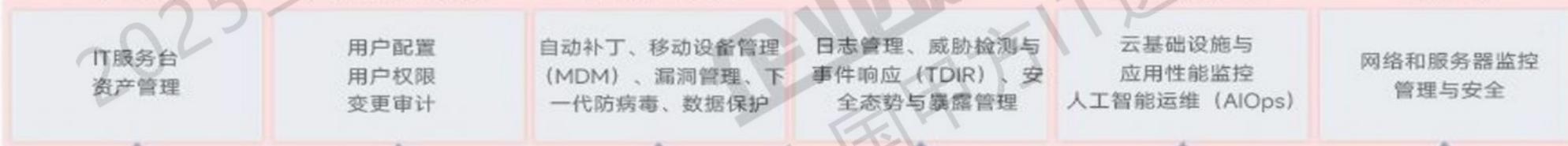


AI助力



运营

受益方：IT管理员

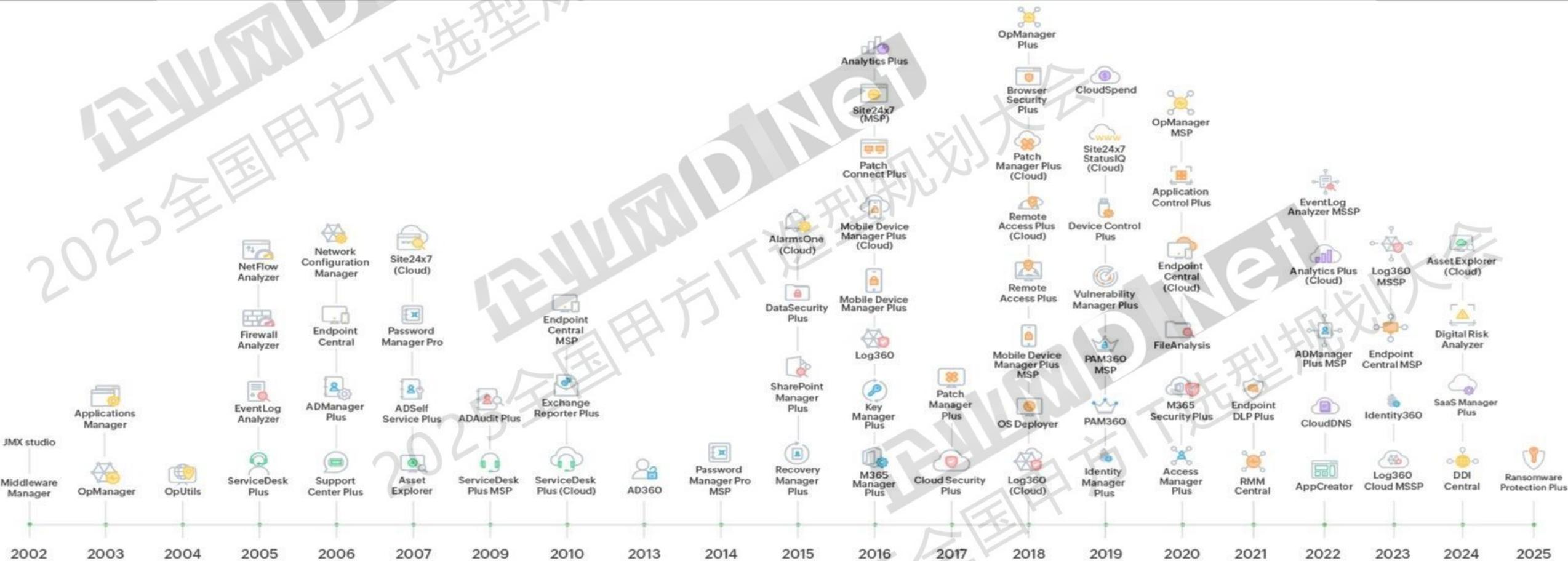


人员

环境

业务

产品演进创新



业界知名咨询公司认可

GIGAOM

OMDIA

Kuppingercoile
ANALYSTS



FORRESTER®

Gartner®

IDC

FORRESTER®



* ISG®

思考感悟

运维是七分靠管理，三分靠技术，体系不在于“先进”，而在于“适配”。

运维的核心不是修问题，而是让问题不发生。

一次故障能修好，靠经验；让它不再来，靠体系。

要拥抱变化，培养既懂传统IT又懂生产流程的“复合型”运维人才。

流程是手段，不是目的；好的流程设计不是环节更多，而是协同更顺。

好的工具，不仅帮助定位问题，更能倒逼流程改进。

感谢您的聆听



公众号

所有软件均开放下载或在线注册方式免费试用!

中文官方网站: www.manageengine.cn