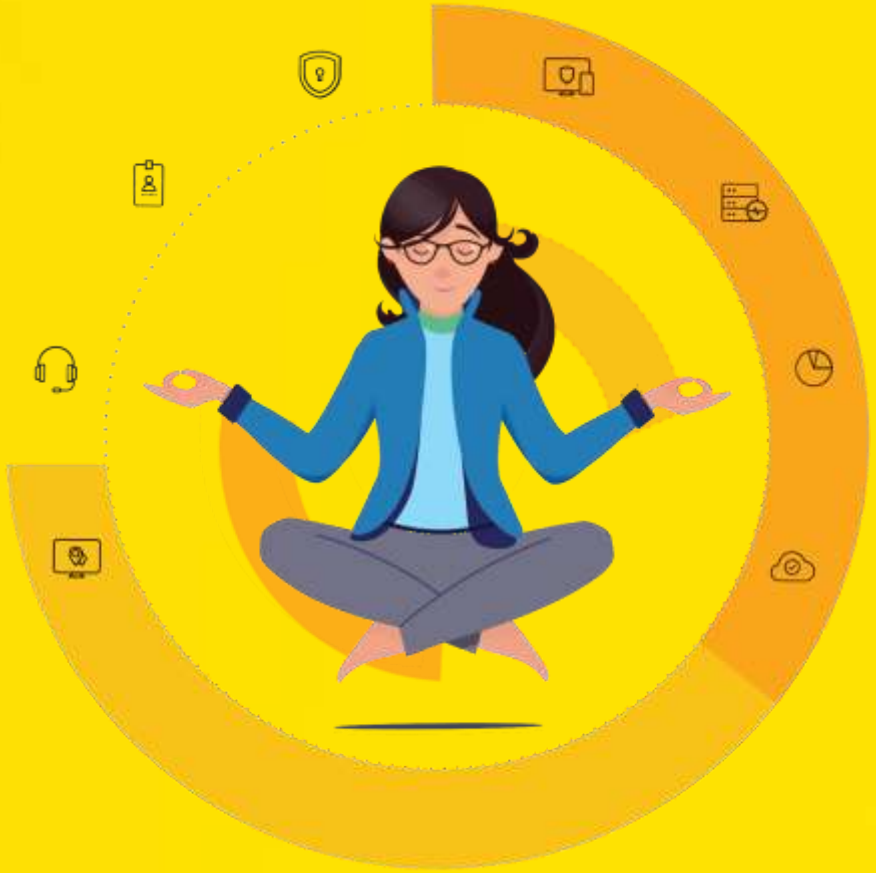
ManageEngine 卓豪

UEM Solution

终端管理
终端安全

IT管理 新体验

软件源自匠心，IT改变世界。
用科技让工作与生活更轻松美好。



IT管理 新体验

为6大洲18万客户提供100多款产品

ManageEngine 卓豪

终端管理+终端安全

终端安全

Vulnerability Manager Plus
检测和修复风险和漏洞的完整解决方案

Patch Manager Plus
满足各种补丁管理需求的一站式解决方案

Browser Security Plus
对全网浏览器进行安全管理的企业浏览器安全工具

Device Control Plus
USB和其他外部设备的控制、阻断和监视一体的DLP解决方案

Patch Connect Plus
让微软SCCM实现对第三方应用自动补丁管理的插件解决方案

Application Control Plus
应程序白名单和黑名单自动生成和维护工具；应用特权管理工具

终端管理

Endpoint Central
管理企业所有终端的UEM解决方案

Mobile Device Manager Plus
移动终端的安全和管理解决方案

OS Deployer
自动磁盘镜像和操作系统部署的综合解决方案

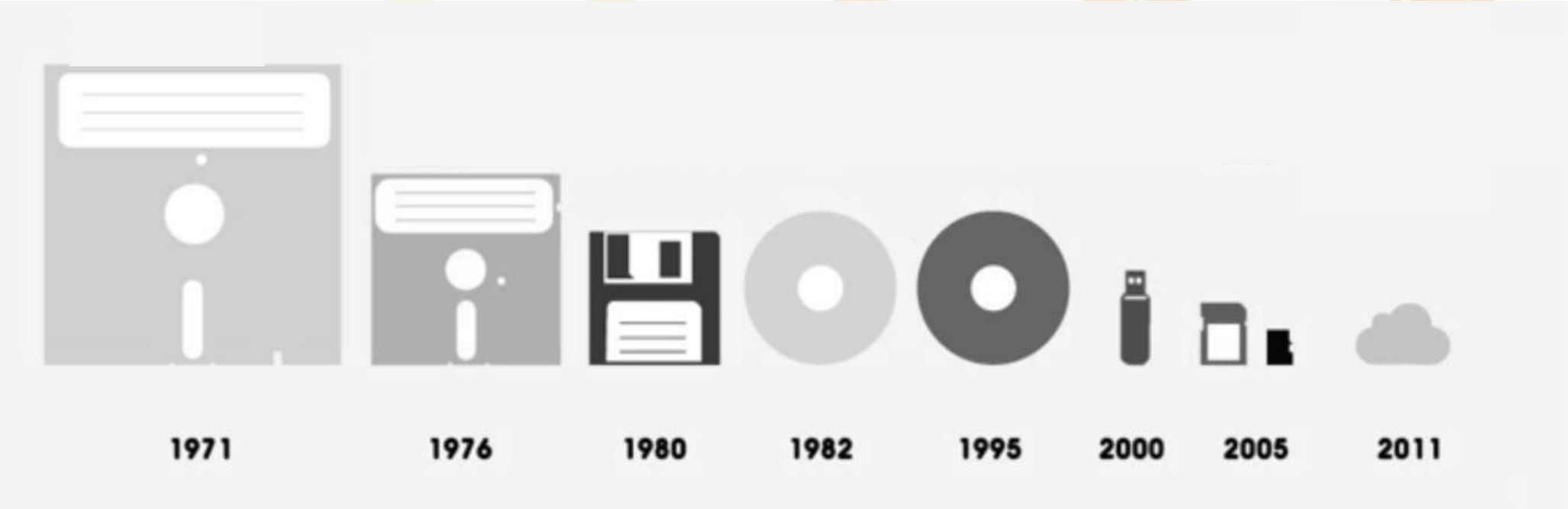
Endpoint Central MSP
适用于服务管理提供商的UEM解决方案

Mobile Device Manager Plus MSP
适用于服务管理提供商的移动终端的安全和管理解决方案

Remote Access Plus
从一个控制台远程管理所有计算机的企业远程软件

https://www.manageengine.cn/desktop-management-solution.html

一切从数字进化谈起


1971
1976
1980
1982
1995
2000
2005
2011

桌面机

笔记本

手机和平板

服务器

销售终端（POS）

浏览器

001,199,620

欢迎进入UEM时代！

（统一终端管理）

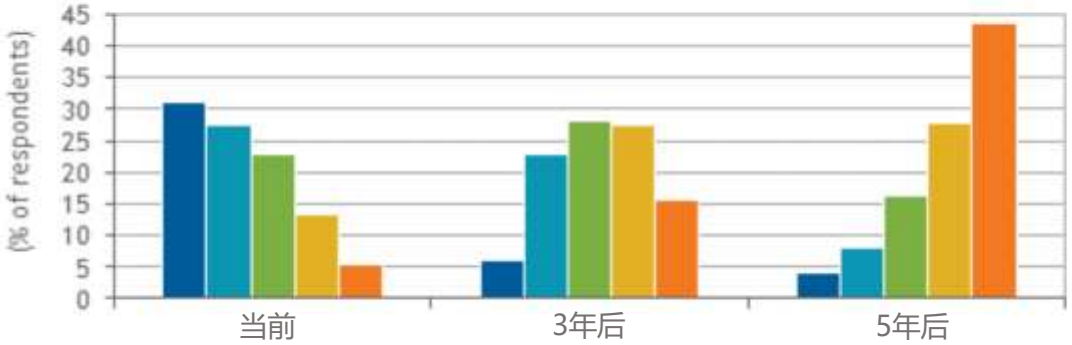
UEM

传统管理和现代管理的平衡

- 传统的终端管理（CMT)
- 移动设备–移动数据 (EMM)
- 现代操作系统管理
- 统一平台的可视化 – 统一终端管理 (UEM)

“统一终端管理采用计划”调查报告

调查：你的组织是如何管理终端设备的，当前的统一终端管理处于什么阶段，5年规划是怎样的?



- 没有统一终端管理：移动设备管理和PC管理是分开的。
- 正引入统一终端管理：开始在一个平台上管理PC（新的和升级的，如Win10）和移动设备。
- 正在添加和更新PC，并主动把已有PC用户整合到统一终端管理平台。
- 大部分设备在使用UEM工具，还有部分设备在使用PC管理。
- 完全引入UEM管理。

n = 500

Source: IDC's *Enterprise Workspace and Mobility Decision Maker Survey*, 2019

Gartner – UEM魔力四象限

Figure 1: Magic Quadrant for Unified Endpoint Management Tools

ManageEngine卓豪

优势：

- 支持的终端种类齐全
  - 微软、苹果和谷歌操作系统
  - Linux各种发现版本 (Ubuntu、Red Hat、CentOS、Fedora、 Mandriva、Debian、Mint、SUSE、Pardus、Oracle Linux及其派生版本)
  - 服务器
  - OEM设备(Samsung、Zebra、Honeywell、Lenovo、Datalogic、Unitech、Nokia、Kyocera、Cipherlab、Seuic和Spectralink)
- 价格优势
  - 极具性价比，比价格第二低的竞争对手还低20%
  - 提供邮件电话聊天等技术支持，还不另收费
- 产品弹性
  - 功能齐全，客户以低投入高收益开启UEM之旅
  - 社交媒体上盛赞其分布式云部署。帮助客户突破了国界和行业的限制。

ManageEngine 卓豪

UEM解决方案

补丁管理

750+应用

漏洞总数带来风险

2016年报出漏洞数：
246个厂家的2136个应用软件中
就有17147个漏洞
Risk Based Security报告

补丁才能制止攻击

在50个最热门的应用中，92.5%
的漏洞在披露的当天提供了补丁
Alpha-gen的2017年漏洞评估报告

应用程序风险不再仅仅是微软

在商业软件中，有86%的漏洞来
自第三方应用程序。
公共漏洞列表（CVE）报告

补丁管理的挑战

- 漏洞数量持续增长
- 现有的漏洞管理方法作用甚微
- 没有时间和资源来及时打补丁
- 不能从企业整体的角度去管理补丁

ME带来的收益

- 减少补丁管理成本
- 减少90%的修补时间
- 综合控制台
- 支持异构环境
- 提高终端安全
- 灵活性和易用性

检测

对终端进行扫描，发现缺少的补丁

测试

为了减轻风险，在部署补丁前进行测试

部署

自动把补丁部署到操作系统和第三方程序

报表

强大的审计。便于管理的可视化报表

配置管理

配置管理需求

- 高效地执行每天的系统管理任务。
- 保护计算机，防止数据外泄和漏洞

40多种预定义配置

- 支持Windows、Linux、Mac
- 基于用户或计算机配置
- USB限制、文件推送、文件/文件夹权限、注册表、防火墙、打印机……

70多种配置模板

- 网络
- 电源管理
- 代理服务器
- 系统工具
- 用户管理
- 硬盘维护
- 控制面板
- ……

批量执行自定义脚本

- 企业脚本库
- 脚本执行授权
- 计划执行
- 执行日志
- ……

100多种脚本模板

- 计算机管理
- 网络设置
- 文件管理
- 浏览器设置
- ……

软件部署

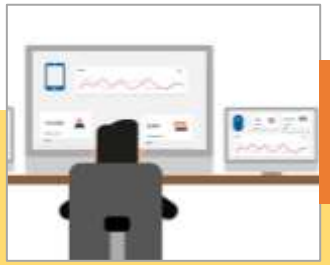
企业需求

- 实现自动化和集中的软件部署管理
- 有效减少服务台中关于软件部署的请求
- 日常软件更新自动化

解决方案

- 软件模板：1100多个内置模板。
- 静默安装：使用同一软件包来安装/卸载。
- 软件库 ： 建立企业自己的软件库。
- 自助门户：用户从企业发布的应用列表中自主安装。
- 部署前后：设置在软件部署前后执行的操作。
- 部署计划：设置计划在非工作时间部署软件。
- 用户身份：可以使用标准用户安装软件。

资产管理



企业需求

- 追踪软硬件资产
- 优化软件许可使用
- 合规性和审计
- 资产报表和告警

解决方案

- 周期性资产扫描
- 硬件保修管理
- 实时资产告警
- 软件使用统计
- 软件许可管理
- 软硬件资产清单
- 文件扫描
- 禁用软件和阻止可执行文件

电源管理

电源消耗

CPU： Intel P4, 2.4 64.6瓦/小时
显示器：50-100 瓦/小时
电价： ¥1.25/KWh*

以一台计算机150瓦。如果全天运行，年费用1642.5人民币
如果只工作日（每周40小时），年费用为375元。
二者相比，费用降低77%

那么2000台，每年可以节省多达253.5万元

- 设置合适的电源管理计划
- 关闭屏幕保护
- 在非工作时间关闭系统
- 电源管理报表

ENERGY STAR

Windows工具

系统管理器

无需登录远程系统即可远程查看被管机器的“任务管理器”、“服务”、“注册表”、“文件浏览器”、“事件查看器”、“设备管理器”、“软件列表”、“打印机列表”；还可以启动“命令提示行”、管理共享、管理用户和组。

远程关机

手动或周期性地远程执行关机、重启、休眠、待机和锁定计算机等动作。可以选择是否经过用户同意才能关机。

局域网唤醒

手动或周期性地远程执行局域网唤醒计算机。

聊天

内置方便有效的即使聊天工具。支持文本、音频和视频聊天。提供记录和审计。

公告

根据需要为特定用户或用户组发送公告消息。

磁盘管理

设置计划执行“磁盘检查”、“磁盘清理”和“磁盘碎片整理”等任务。

移动设备管理

应用管理
创建企业应用目录；分发应用；应用黑白名单...

安全管理
强制密码访问；远程锁定；实时位置追踪；数据擦除

策略管理
配置和下发策略；限制摄像头；配置WiFi VPN 邮件...

内容管理
创建文档内容库；分发不同格式文件；限制向未管设备共享

邮件管理
利用设备集装箱化和Exchange ActiveSync管理邮件内容和账户。

集装箱化
在BYOD上区分管理和保护个人数据和公司数据

Kiosk模式
锁定设备运行单一应用，或指定的几个应用。

审计和报表
追踪和分享资产信息，帮助您保护公司敏感数据。

资产管理
追踪和分析设备信息；获取设备的应用、证书等信息；
远程故障排查。

地理围栏
追踪设备位置，限制设备在指定的物理区域内使用。

操作系统部署

自动化

降低成本

系统标准化

提高效率

创建

使用高级的技术在线或离线创建镜像

定制

按照用户的角色和部门做系统定制

部署

批量将系统部署到计算机

实时镜像

可以把网络中正在使用的机器做成镜像，不影响当前用户使用。

统一部署

使用相同的身份验证密码做统一的简单的部署，和传统手动方式说再见。

和硬件无关

为所有计算机部署标准化的系统，为不同厂商型号的计算机配置和安装驱动。

定制部署

按照需要定制镜像。还可以在部署系统后统一配置和安装软件。

部署到各处

可以在一个中心位置为不同分公司部署系统。

多种引导方式

选择你方便使用的方式引导，例如IOS、USB、PXE。

浏览器安全

检测和管理漏洞

- 浏览器使用趋势可视化
- 发现网络中所有的插件
- 检测插件中的安全漏洞
- 管理和确保插件的安全

强制安全策略和确保合规性

- 在计算机上部署配置，防止浏览器导致的安全风险。
- 确保满足安全合规性。
- 确保企业数据安全。

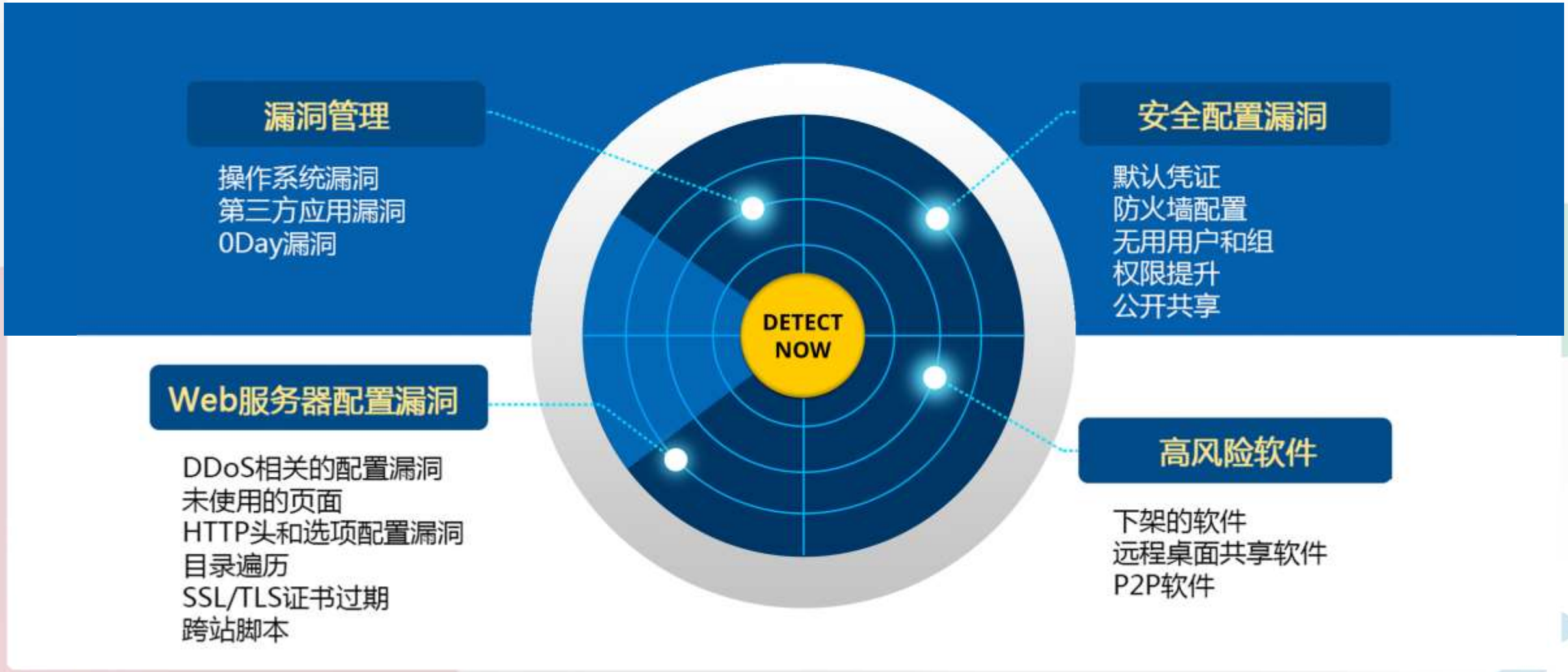
审计和生成报表

- 持续跟踪浏览器的健康状态。
- 检测和发现插件漏洞。
- 生成安全信息报表。

控制浏览器插件、扩展和站点

- 根据业务需求来授权Web应用的访问。
- 锁定浏览器只允许员工访问信任的Web应用。
- 在浏览器上隔离企业和非企业站点。

漏洞管理


漏洞管理
操作系统漏洞
第三方应用漏洞
0Day漏洞
安全配置漏洞
默认凭证
防火墙配置
无用用户和组
权限提升
公开共享
DETECT
NOW
Web服务器配置漏洞
DDoS相关的配置漏洞
未使用的页面
HTTP头和选项配置漏洞
目录遍历
SSL/TLS证书过期
跨站脚本
高风险软件
下架的软件
远程桌面共享软件
P2P软件

远程控制

高级远程控制

支持网络终端各种计算机

符合HIPAA法案要求的桌面管理软件，支持Windows、MAC和Linux。包含10余种特色功能。

系统管理

借助10余种实用工具快速解决问题

远程管理服务和进程、命令提示行、注册表、管理用户、文件、共享和打印机等。

视频和音频聊天

和技术员或用户即时沟通

在远程处理问题的过程中及时和用户或技术员通过视频、音频和文本方式进行交流，带来无缝协作体验。

局域网唤醒

可以立即启动远程计算机

查看代理信息， 按照需求来启动远程计算机。轻松一点就可以启动一台或多台计算机。

远程关闭

有效节约运行成本

掌握哪些计算机没有活跃用户，并执行远程关闭、锁定和休眠。可以批量执行。

审计和报表

用于审计的实时报表

记录所有的远程会话信息、包括聊天记录、对远程机器的更改等。

应用控制

传统方式

- 应用列表的创建和管理是一个冗长的过程。
- 应用控制有可能影响到操作系统关键功能的使用。
- 缺少实用性和灵活性
- 识别和解决灰名单应用非常困难

安全风险

应用程序几乎成了安全风险的同义词。
根据NVD的数据，过去10年，和应用相关的安全问题增**273**%。

生产力下降

应用程序导致的生产力下降。
即时消息和游戏类的应用程序在各种工作场所起到了**反作用**。

特权攻击

最容易引起攻击，而且常常被忽视。
Forrester评估报告指出：**80%**的安全故障都和特权凭证有关。

管理难度大

应用程序越多需要管理的补丁也越多。
限制运行那些真正需要的程序，会使IT管理工作的**范围和难度**大大增加。

应用控制

- 为企业提供了掌控有风险的软件厂商的手段。
- 灵活的管理模式满足不同企业和场景的需要。
- 管理绿色软件，实现全面精细管理。

应用白名单

通过厂家、产品名称、是否验证、文件哈希等定制灵活的规则来自动创建软件白名单。

应用黑名单

限制非业务相关应用和恶意执行程序，阻止影响生产力的应用，控制攻击风险。

灵活的管理机制

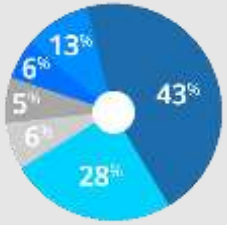
审计模式允许白名单和灰名单程序运行；严格模式只允许白名单应用运行；灵活地管理应用名单。

终端权限管理

按照需求来分配特权访问。防止因为权限过高引起的攻击。

外部设备控制

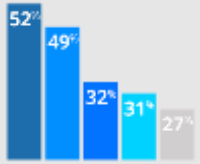
安全现状



来自内部的安全风险

90%组织感到很容易受到内部威胁

如今在组织中发生数据泄露的数量正在急剧上升。其中一个主要原因是对用户和设备授予的访问权限过大。



数据处于风险中！

限制不必要的数据移动、删除和修改。

不同数据受攻击程度：账户数据（52%）、敏感的个人数据（49%）、知识产权（31%）、员工数据（31%）、运营数据（27%）

$8.76 million

average yearly cost of insider threats.

企业的损失

来自内部的安全风险给企业造成了大量的损失，平均每年876万美元的损失。

需求

数据丢失

内部员工攻击

外接设备攻击

合规性问题

- 审计谁使用什么设备
- 识别并控制恶意设备
- 识别恶意风险并解决

设备控制

设备和端口控制

- 控制、阻止和监控移动设备
- 包括：移动存储设备、鼠标、生物识别、打印机等11种设备。

文件访问控制

使用基于访问控制策略的严格规则防止数据丢失 - 设置只读权限，阻止外设拷贝数据等。

文件传输控制

阻止未授权的数据传输，根据文件类型，文件大小限制文件传输。

受信任设备列表

- 创建排除设备策略，将其添加到受信任列表。
- 当未授权的设备插入终端接收告警通知。

临时访问

- 针对要访问的数据，授予设备临时访问权限
- 终端用户发出临时访问请求，通知所有技术员

报表和审计

- 设备，用户，被管设备的报表
- 查看所有设备行为和文件传输
- 计划报表

ManageEngine 卓豪

UEM产品

桌面管理

- 补丁管理
- 软件部署
- 资产管理
- 配置
- 远程控制
- 电源管理

移动设备管理

- 设备管理
- 应用管理
- 安全管理
- 邮件管理
- 内容管理
- 集装箱化

操作系统部署

- 操作系统镜像
- 操作系统部署
- 通用设置部署

现代管理

- 位置追踪
- 公司/完整擦除
- KIOSK模式
- Windows商店应用分发
- 配置文件分发
- 通过SCEP分发凭证

我们为您提供

Endpoint Central
桌面管理

Mobile Device Manager Plus
移动设备管理

Patch Manager Plus
补丁管理

Browser Security Plus
浏览器及其安全管理

OS Deployer
操作系统部署

Endpoint Central MSP
适用于MSP的桌面管理

Device Control Plus
USB和外围设备管理

Application Control Plus
应用控制管理

Remote Access Plus
远程访问工具

Vulnerability Manager Plus
企业级漏洞管理

TOYOTA
unicef
xerox
BRIDGESTONE
pwc
SHANGRI-LA HOTELS and RESORTS
CISCO
Honeywell
WELLS FARGO
HARTFORD PUBLIC SCHOOLS
IBM
CSD
Parker
AT&T
Bell Helicopter
CENGAGE Learning
ao.com
Cognizant
CSS CORP
DAI Shaping a more livable world.
DHL
Dunelm
fiserv.
flydubai
FOUR SEASONS Hotels and Resorts
FOX
BMI Healthcare
MetLife
mondi
packnstack
Raytheon
Spectrum
SYNEXUS
TATA TATA CONSULTANCY SERVICES
VANGUARD
verizon
XPO Logistics
Pfizer

评 价

认 可

ManageEngine连续多年进入

Gartner统一终端管理魔力四象限

ManageEngine也多次获得统一终端管理的“客户之选”称号

集　成

ManageEngine ServiceDesk Plus

Jira Service Desk

zendesk

spiceworks

ManageEngine AssetExplorer

servicenow

ManageEngine
ServiceDesk Plus

集成IT服务管理，实现终端自动运维

提升用户体验

在统一控制台中处理移动设备管理的相关工单。
保障服务级别协议。

收集IT资产

通过轻松点击即可共享IT资产数据。
在一个中心管理细颗粒度的IT资产。

资产告警和追踪

便利的资产审计和追踪功能。
将黑名单应用告警记录为ServiceDesk Plus工单。

完全的UI集成

终端管理和IT服务管理系统完全集成在一个界面中。

终端管理自动化

从ServiceDesk Plus界面管理软件分发和资产管理。
自动化终端管理服务流程。

ManageEngine
Analytics Plus

终端管理和安全的透视

预置的透视报表

Analytics Plus内置了终端安全的深入透视报表和仪表板。

IT管理全景可视化

把其他IT管理工具的数据集中展示在一个仪表盘中。

AI+敏捷

通过拖拽生成各种类型的报表和图表。
人工智能自动生成报表；智能助理用透视报表回答您的问题。

动态分析

切片试的动态数据展示，实现了终端风险的即时可视化。

实时合作

实现终端管理的趋势分析、预测规划、实时全屏、动态共享等。

ManageEngine 卓豪

IT管理 新体验

www.manageengine.cn