ManageEngine 卓豪
Endpoint Central

案 例

与某全球制造商的十年合作：

对抗勒索软件，保障产线安全

客户介绍

这些年全球经济受各种因素的影响，一个企业如何在全球范围内进行有效的运营是企业和消费者共同关注的焦点。在汽车领域也是如此。该客户就是从事汽车零部件制造的全球企业。我们根据客户的要求，在本案例中对所有名称和地点进行匿名处理。

制造业

管理的终端：2万5千

全球各地有分支机构

通过 1 个控制台

Endpoint Central帮助客户管理

超过 2万5千 个终端

涵盖 350 个分支机构

在 41 个国家和地区

提供安全保护

员工的办公环境

产品线的服务器基础架构

我们帮助客户取得了哪些成就？

01

通过观察使用模式，优化了软件的投资。这些软件用于产品生产和设计，价格昂贵。

02

在不影响生产力的情况下，降低了办公终端和生产服务器的安全风险。

03

实现不同时区用户登录时间可视化，进行了广泛的电源管理以满足环境、社会和治理（ESG）目标。

04

2012年，制造商部署了Endpoint Central，统一了多个活动目录（AD）环境和工作组的终端，横跨多个部门和时区进行管理。

05

2016年，在全球Wannacry攻击期间，他们在仅36小时内修复了所有设备，包括服务器。

06

保护高管和远程员工笔记本上的机密设计资料和生产文件。

07

用统一平台取代了分散的解决方案，降低了管理投入，提升了管理效率。

08

平台的可扩展性使他们能够适应终端的增长速度。实现与其技术栈的集成，让现有投资价值最大化。

案例研究的内容包括：

- 一切开始于可视化
- 战情室中的36小时
- 保护生产服务器：安全与可用性之间的平衡
- 应对挑战：可持续性、安全性及更多

一切开始于可视化

在本案例研究中，我们采访了这家汽车制造公司的IT资产管理（ITAM）和安全业务负责人。十年前，他们寻求解决资产管理挑战的解决方案。那时候他们正在全球扩展，不断在新的城市建立新工厂来支持当地客户，这期间还发生了多次收购和成立合资公司。这样，各处IT部门独立运作，IT系统也各自独立。问题是，随着公司的扩展，这种去中心化的方式让IT管理变得越来越低效。为了解决这一问题，公司设立了技术和工业解决方案部，来为各地分支机构提供集中式的IT支持。

ITAM和安全团队将ManageEngine卓豪的Endpoint Central作为这一转型过程中的关键系统进行部署。Endpoint Central从分散在各地的AD环境和工作组中聚合资产数据，提供实时更新，确保分支机构管理员能够及时获得添加或移除设备信息。如今，ITAM和安全团队负责管理超过25000个终端，涵盖350个分支结构，包括制造工厂的服务器、员工办公和远程办公环境。

> “今天，就在我们谈话的同时，有五台新笔记本电脑已加入某个工作组。从治理、风险和合规的角度来看，获取终端变化，获得资产可视化是至关重要的。”

终端管理可视化已经转化为切实的价值。这家制造企业在其概念和产品设计中高度依赖昂贵的软件。借助ManageEngine平台，他们实施了有效许可管理，以优化软件支出。这包括对员工设计软件使用模式的实时分析，以识别许可数量短缺或过量。他们还高效地管理未使用的许可，并可以主动跟进合同续签任务。Endpoint Central使这家制造企业能够掌握软硬件资产的实时库存，记录安装历史以备审计使用。此外，他们对合规性的要求的实现，通过ISO审核等得到了进一步能力增强，实现了全流程管理。通过基于角色的访问控制，审计人员获得了对其资产收集数据的只读访问权限，包括终端暴露和安全状态的分析。对于移动设备管理（MDM）也实现了同样的设置。将包括移动设备、服务器和台式机在内的终端信息集中在一个地方，显著增强了审计人员的信心，有力支持了公司业务在全球的开展。

“通过使用Endpoint Central所获得的信息和响应能力，使我们的团队在面对各种审计时保持信心，并使我们的技术投资价值最大化。”

战情室中的36小时

2016年是我们与这家制造业公司合作的关键时期。这也是Wannacry网络攻击让IT界人心惶惶的时刻。那天一早，IT资产管理（ITAM）和安全负责人接到了首席信息官（CIO）的电话，这一通电话将永远改变他们的补丁管理方法。他们的整个IT团队聚集在一个战情室内，制定应对攻击威胁的行动计划。ITAM和安全负责人提出，由于Endpoint Central的客户端在所有终端上运行，他们可以利用现有基础设施为其全网计算机打补丁。IT团队在少数几台计算机上进行了测试，进展顺利。

> “我们在房间里待了36小时。当我们在两天结束时终于看到补丁合规小部件上呈现完整的绿色图表时，我们松了一口气。这是我们第一次使用Endpoint Central为整个系统打补丁，包括服务器。考虑到我们的运营规模和复杂性，这是一项巨大的成就。”

当时部署补丁管理策略的概况：在接下来的36小时对该公司的IT团队来说是一场紧张的马拉松。他们在战情室内，利用Endpoint Central为遍布全球的远程站点打补丁。

IT团队的安全战略结合Endpoint Central的可扩展性，不仅抵御了全球威胁，还将危机转化为增长的机会。通过与Endpoint Central的成功合作，IT团队更有信心，创建一个专门的小组，把终端管理扩展到了生产线环境中，就像办公环境和服务器基础设施中一样。

保护生产服务器：
安全与可用性之间的平衡

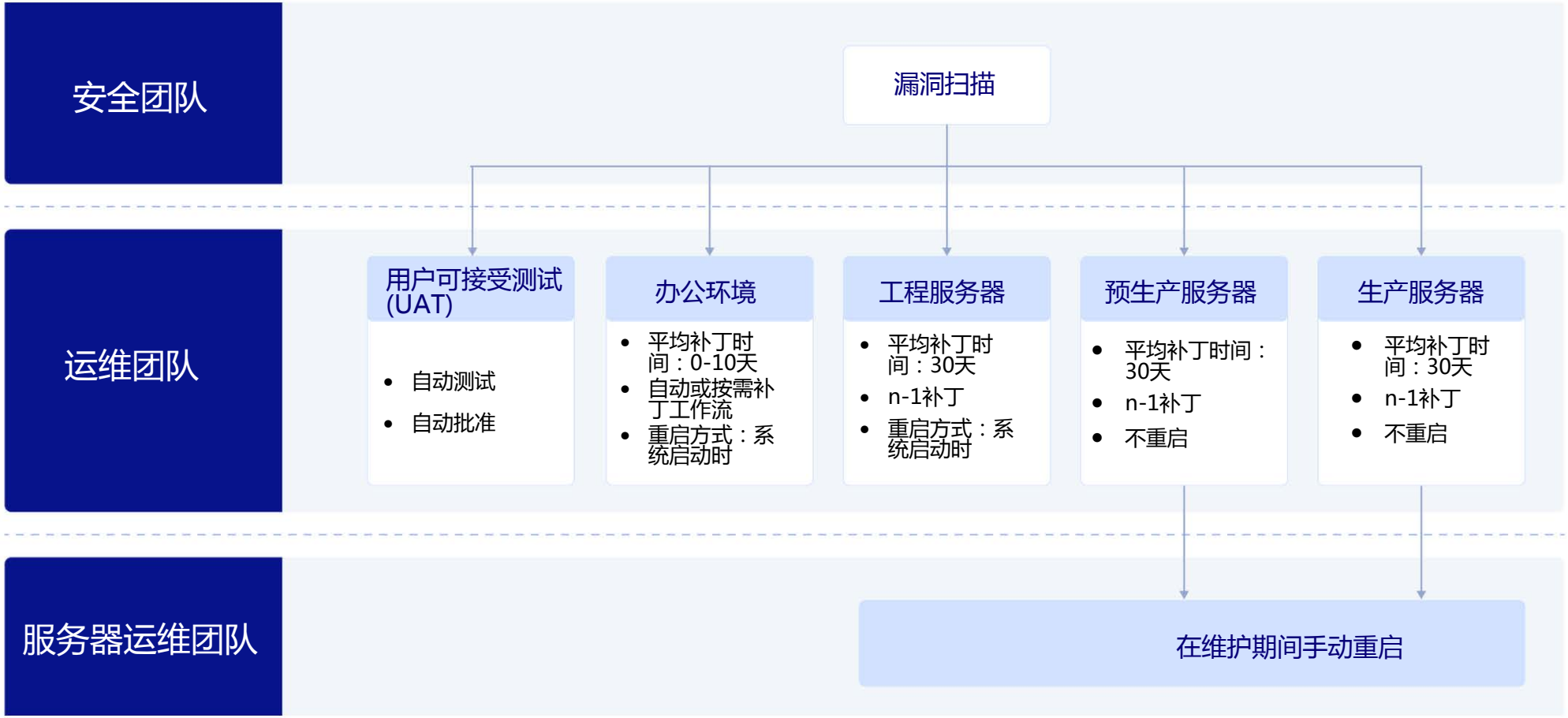
在他们的制造工厂中，生产机器是他们运营的支柱。这些机器由服务器控制，服务器存储了即将由原始设备制造商（OEM）推出的新车型的机密设计、生产计划文档和其他知识产权。他们在2016年的经验使他们深刻意识到修复这些服务器的漏洞以防止勒索软件攻击的重要性。

然而，服务器的可用性是他们安全运营的一个障碍。这些服务器上的软件和数据库在向生产机器提供设计和工作数据、以及监控生产活动。为这些服务器打补丁是一个挑战，因为这些服务器不能轻易重启。如果一台服务器宕机，生产将会停止。对于这家制造组织来说，这在严格的生产时间表下是不可接受的。

“对此进行一些分析，如果我们在一周内需要交付一款产品，如果仅仅宕机几小时，这就会影响我们的生产成本和生产计划。让生产机器重新启动需要时间。因此，挑战在于，他们无法依据我们的要求随意在生产环境中重启服务器。”

该公司采用业界补丁管理规范作为其补丁管理的操作手册，这个管理过程需要可靠的工具、部署策略，以及和不同环境的相关者进行沟通。

以下是所采用的补丁管理策略的概述：



为办公环境打补丁是日常工作，他们可以在全球范围内按需处理紧急操作系统更新，SLA为2-5天，而标准补丁周期仅需10天，这都得益于我们的Endpoint Central的自动化功能。

他们采用基于测试的补丁流程，首先在小规模上测试补丁，然后进行自动审批，逐步在办公环境中推广。所有用户设备在几天内完成一次补丁部署。

对于服务器的补丁管理，和对PC的管理是很不一样的。这个企业通过Endpoint Central获得了2万5千个终端的集中和实时的数据。这是执行集中管理和采用差异补丁管理策略的基础。这些Endpoint Central获得的的资产信息定期录入到他们的内部配置管理数据库（CMDB）中。各个生产工厂管理员为每台服务器添加了标签，以明确是什么类型的服务器，属于工程、预生产或生产环境。对于生产服务器，他们需要服务器配置、正在运行的应用程序和数据库的信息，并记录其所有者。这些CMDB信息在规划管理和维护策略的时候，例如打补丁，是至关重要，帮助他们确定相关人，沟通和确认服务器维护时间。

他们的标准做法是为生产和预生产服务器保持N-1软件版本，其中N-1表示一个月前的软件版本。通过我们的平台，他们可以保留最近三个月的已替代补丁。他们在将补丁安全地推广到生产服务器之前，会在测试组上进行30天的最新补丁行为检测。

Endpoint Central的部署策略可以选择不同类型的服务器，并进行配置，不对这些服务器的重启。服务器操作员随后在预定的停机时间内手动执行重启。

> “一个好的安全解决方案需要实现管理的平衡点——也就是说，要设置一个可接受的风险水平，以达到保障业务的目标。”

安全团队每月与漏洞风险系统（Tenable）进行例行审计，以验证系统是否存在漏洞，并与IT运维团队就审计结果进行讨论。为了充分利用现有投资并简化漏洞响应流程，IT团队正在探索Endpoint Central与Tenable的集成方案。

尽管Endpoint Central的安全版包含一个专有的漏洞管理模块，但Endpoint Central的可扩展和集成能力通过集成已有系统，帮助这家企业能够最大限度地从当前投资中提取价值，最终降低他们的总体成本。

应对挑战：
可持续性、安全性及更多

随着公司的壮大和业务的发展，IT管理要面对设计师和工程师远程工作带来的进一步终端管理和安全的挑战。员工们一般在办公室内有桌面电脑，随身携带笔记本电脑用于漫游办公，这就需要从个人笔记本电脑连接到这些位于办公室的桌面电脑。为此，他们采用了ManageEngine卓豪PAM 360，这是一种经济实惠的解决方案，提供安全的远程连接。

另外一个挑战，制造业非常关注能源节约，需要管理终端在不活动期间的电源计划，以符合其环境、社会及治理（ESG）目标。为了解决这个问题，IT团队有效利用Endpoint Central收集了350个地点的用户登录报表。该数据对于规划电源管理时间表至关重要。利用平台的远程管理功能，他们高效地将不活动的桌面电脑休眠，并按各个时区的登录和工作时间表设置批量计算机的关机计划。这一贡献加强了该企业成为其行业中全球首选可持续解决方案提供商的能力。

以前，该公司将大部分敏感数据存储在与互联网隔离的生产服务器和中央存储系统中。只有少数高管会在公司网络之外使用这些数据。随着大多数员工转向远程工作，这些敏感更多会直接暴露于互联网，他们的攻击面大大扩展。对于IT来说，保证生产力和数据安全的平衡变得挑战重重，需要管理机密的设计和生产计划文档在终端上的本地存储。为了解决这一问题，Endpoint Central发挥了关键作用，通过启用BitLocker加密在其不同位置的设备上保护敏感数据。即使员工休假或长时间离线，我们的平台也安全地备份BitLocker恢复密钥，从而简化了加密管理过程。

携手同行

在ManageEngine卓豪二十多年的行业历程中，像这样的制造企业与我们的伙伴关系是我们存在的重要组成部分。当他们开始与我们合作后，就迅速认识到我们是为了长远合作提供产品和解决方案的。我们凭借完全自主开发的方式，在一个平台上开发了所有功能，从来不依赖收购去堆砌功能。我们稳定的产品结构，提供了可靠的扩展能力，这样这家公司就使用Endpoint Central应对终端的增长速度，而且终端管理和安全流程更加成熟。

通过和我们的合作，他们成功整合了孤立的工具和流程。他们逐渐替换了多个工具，如用于补丁的WSUS、操作系统部署系统、移动设备管理和远程控制（使用TeamViewer）。这一举措大幅减少了管理开销和IT投入。

随着勒索软件和数据泄露威胁的增加，这些威胁占今天网络攻击的70%以上，该公司开始使用我们的“新一代防毒”模块。“新一代防毒”可以主动应对勒索软件的攻击，保护和恢复数据；通过基于机器学习的恶意行为管控，来提高终端的安全。

展望未来，该公式正在进一步评估这些新的功能，强调了他们对我们作为长期合作伙伴的信任，能够满足他们今天和未来的需求。

联系我们

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。

产品演示