[趋势科技成功案例]

云铜股份冶炼加工总厂与病毒争分夺秒
趋势科技 Deep Security 为安全生产保驾护航

随着中铝云铜股份冶炼加工总厂（集团）有限公司（以下简称：云铜股份冶炼加工总厂）企业规模与信息化应用的不断扩展，其内部的安全生产规范、业务特点都对自身的网络安全提出了更高的要求。为积极应对日益严峻的病毒与黑客威胁，云铜股份冶炼加工总厂携手全球服务器安全、虚拟化及云计算安全领导厂商——趋势科技，在不变动现有安全框架的前提下，使用趋势科技服务器深度防御系统（Deep Security）为企业信息服务器群提供全面的安全加固，在补丁管理与未知病毒防御方面都收到了令人满意的效果。

传统主机防毒系统无法有效保障生产服务器安全

随着云铜股份冶炼加工总厂有色金属业务的快速发展，服务器数量和网络规模不断扩大。据了解，目前云铜股份冶炼加工总厂服务器尚未实施统一的安全防护架构，各自为政的生产系统不但对外接口众多，且系统安全防护水平参差不齐。这些服务器所承载的核心业务包括了生产控制、等诸多数据，一旦出现病毒和黑客入侵的情况，必然会影响的业务处理，生产安全也可能受到破坏。而且，在云铜股份冶炼加工总厂原有的服务器安全防护架构中，只采用了传统防病毒软件作为主机层面的防护手段，在日益变化的威胁面前，补丁管理和未知病毒防护的问题逐渐凸显出来。

当前大部分黑客入侵、木马注入等威胁，大多是基于操作系统及应用程序的安全漏洞进行攻击。因此，为服务器及时升级系统及应用程序补丁是防御新形态攻击、保障服务器安全的唯一途径。但安装补丁之后，管理员必须重新启动服务器才能使补丁生效，这就使得服务器对业务系统无法提供连续性的服务。另外，由于云铜股份冶炼加工总厂具备大量定制开发的业务，各厂商发布的安全补丁并不能保证能够与每个业务皆兼容，一旦发生因为安装补丁而导致的业务访问中断问题，“回滚”的难度极大。

另外，即使云铜股份冶炼加工总厂已经采用了网络版防病毒软件，服务器依旧会遭受未知病毒、木马的威胁。究其原因，这时因为传统防病毒产品是采用病毒特征库的技术，而未知病

毒并不存在病毒库的黑名单中，所以即使服务器部署了最新的病毒特征库，也不能及时发现未知病毒的入侵。仅当未知病毒已经对生产业务带来实质影响时，IT 部门才能对未知病毒事件作出响应。但最佳的处理时机已过，IT 部门需要投入大量的人力、时间成本才能修复未知病毒带来的损害。因此，对未知病毒的提前发现及处理，亦是云铜股份冶炼加工总厂 IT 部门非常关注的技术难点。

要走出困境，云铜股份冶炼加工总厂就需要在找出一种创新性的服务器安全加固方案，不但要确保服务器得到最新的系统及应用程序补丁保护，同时也能为生产服务器提供实时的，针对未知病毒入侵监控机制。

Deep Security 提前一步阻断威胁 虚拟补丁让生产系统永不中断

在对市场上主流的服务器安全防御系统进行了充分评估之后，云铜股份冶炼加工总厂的 IT 技术部门最终决定使用趋势科技 Deep Security 作为全网生产服务器安全加固方案，以解决上述问题。

当前，所有基于漏洞进行的攻击，其数据包中必定包含特定的指令。当目标服务器具备某种特殊的应用并收到这种数据包时 ,就会因为执行了这些特定的指令而使攻击者获取管理员权限，进而被控制。基于这种攻击的原理，Deep Security 的深度包检测技术实现了在这些攻击数据包达到服务器之前，就进行内容检查和拦截的功能。该功能可以通过漏洞攻击规则及智能规则对数据包包含的指令进行比对，一旦发现有数据包触发安全规则，就可以根据预定的策略进行监控、丢弃或阻断的动作，保障服务器的安全。

据了解，对于已知的漏洞，Deep Security 为云铜股份冶炼加工总厂内部运行的各种应用程序提供开箱即用的漏洞防护，使其免受了多次的漏洞攻击。对于最新发现的漏洞，Deep Security 能够在第一时间提供虚拟补丁策略，在无需重新启动操作系统的前提下，即可在数分钟内将这些策略应用到所有的服务器上。在不中断生产业务服务器的基础上，为云铜股份冶炼加工总厂生产服务器提供最新的系统及应用程序补丁保护。

另外，当未知病毒入侵系统时，必然会修改系统中某些重要的文件，以此达到获取系统控制的目的。为了防范病毒对系统的修改，趋势科技 Deep Security 的完整性监控模块实现了对生产服务器的系统文件、目录、注册表项、注册表值以及已安装软件和运行的服务中发生更改的扫描和监控。一旦上述的关键位置发生恶意修改的事件，Deep Security 即实时生成告警，通知管理员对高危服务器进行诊断，及早处理未知病毒，降低未知病毒对业务带来的风险。

趋势科技 Deep Security 系统能够通过不重启操作系统的方式修复系统及应用程序漏洞，有效解决了困扰多年的服务器补丁管理难题。另外，通过完整性监控技术为生产服务器提供未知病毒的实时监控能力，让安全防护跑赢了病毒滋生的速度，真正使 IT 部门对生产服务器的安全运行能做到心里有数。在过去的 2012 年，云铜股份冶炼加工总厂全网都没有发生因病毒造成的生产事故，这受到领导和用户层的一致认可。“

###

关于趋势科技（Trend Micro）

趋势科技是全球虚拟化及云计算安全的领导厂商，致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问：www.trendmicro.com.cn。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。