TREND MICRO™ Securing Your Web World

抵御MS12-020，趋势来帮你

微软提醒

所有企业IT管理者

立即针对MS12-020

“微软远端桌面协议漏洞

可允许透过远端连接来执行本机程序“

影响所有Windows版本的

安全漏洞更新

采取行动

Windows RDP高危漏洞

- MS12-020
- 影响范围：所有Windows 服务器和桌面系统
- 具体影响：
  - 允许执行远程代码，无需身份验证
  - 有一段POC（攻击概念证明）代码被公布
  - 趋势科技已发现一个黑客工具可以攻击该漏洞，检测名为DDOS_DUCAU.A
  - 前还没有收到利用该漏洞传播的病毒

微软的建议

- 安装关键更新
- 该漏洞是针对RDP的攻击，因此没有开启RDP的系统，将不受影响
- 对于无法立即部署补丁的用户，关闭RDP服务、从防火墙上禁用3389端口或者监控3389端口。

趋势科技解决方案

- TDA、DS、OSCE等产品都有针对该漏洞的解决方案
- 截至到3月20日，发布了以下特征码
  - TDA 特征码
    - NCIP PATTERN 1.11597.00
    - NCCP PATTERN 1.11581.00
  - NVP (NVW/OSCE)
    - 110314
  - Ti5
    - Ti5 RR 1.10021.00
    - NVP 1.10021.00

TREND MICRO

终端层: OfficeScan 10.6 - IDF
业界第一入侵防护防火墙模块

漏洞屏蔽，无需打补丁，立即防护，业务应用不中断

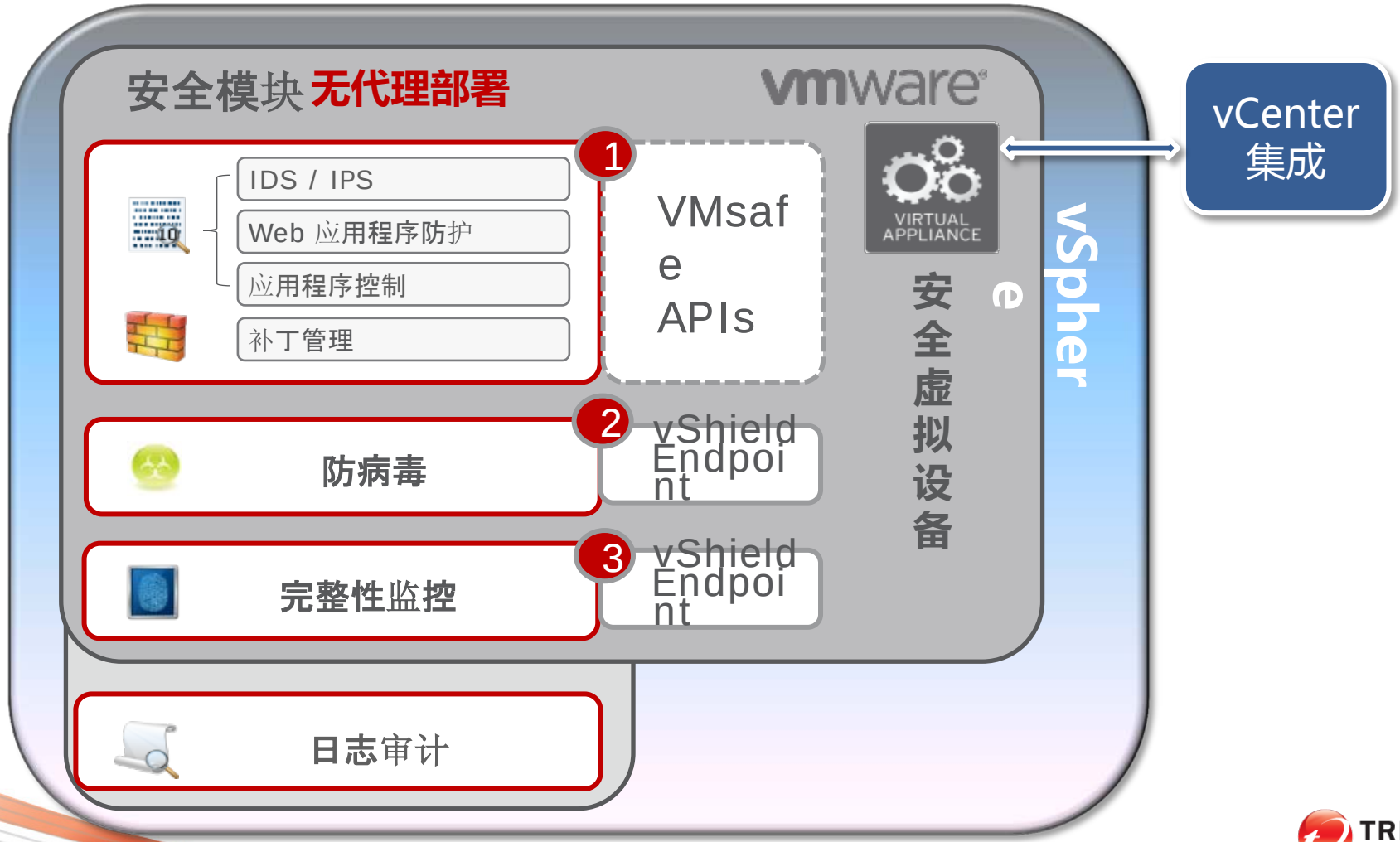
Microsoft 安全公告 MS12-020 - 严重

远程桌面中的漏洞可能允许远程执行代码 (2671387)

- 虚拟补丁
  - 巡检遗漏补丁和存在安全漏洞
  - 操作系统
  - 常用桌面应用
- 推荐轻巧，简易部署的安全策略
  - 非侵略式完成补丁效果，填补安全漏洞
  - 零日攻击防户
  - 报告尝试利用漏洞的攻击
- 补丁安装后相关规则自动卸载

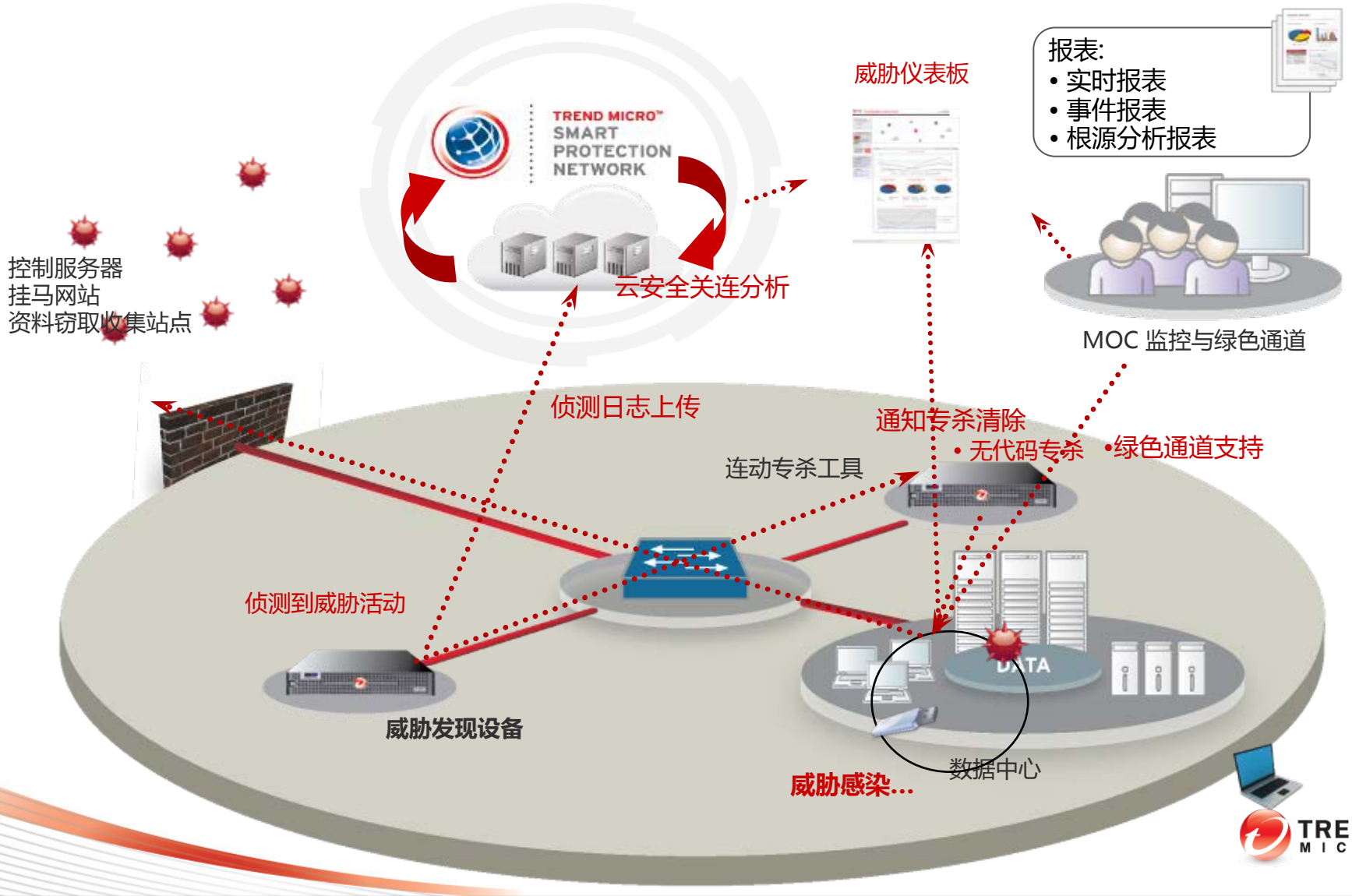
TREND MICRO

虚拟化无客户端底层防护：DeepSecurity



TREND MICRO

威胁治理解决方案：TDA-NVWE



谢谢！

TREND MICRO