McAfee
Together is power.

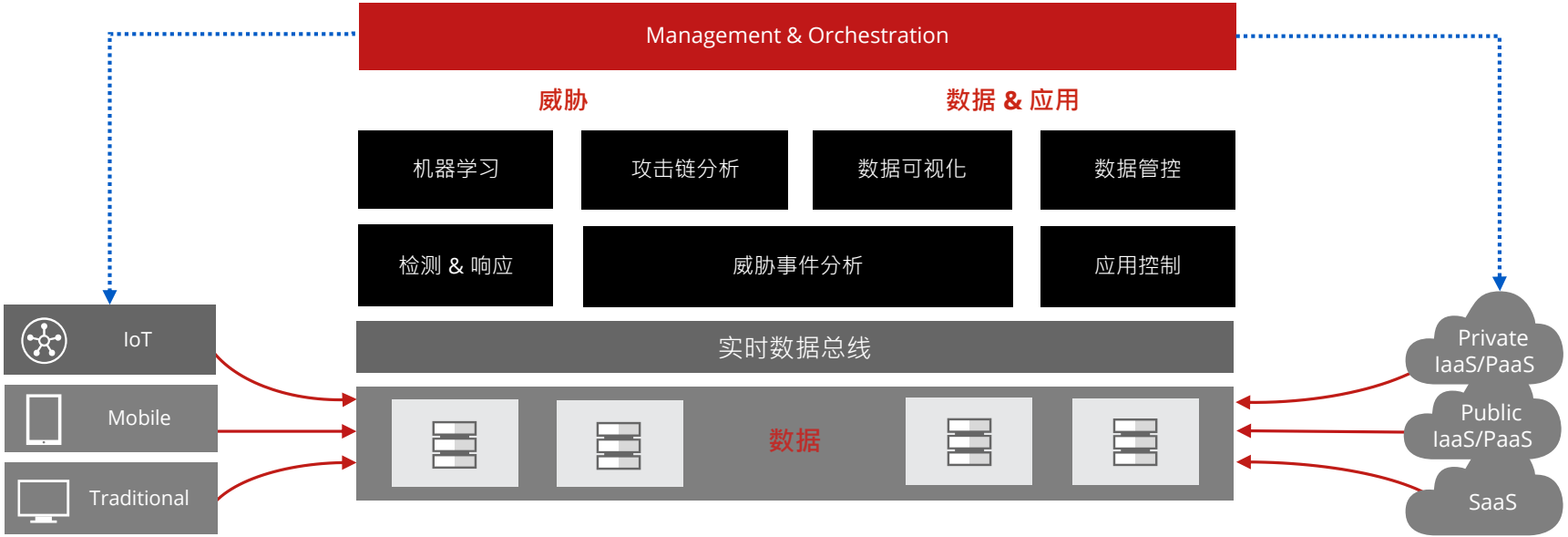
咨询订购：400-010-8885、 Support@mcafees.com.cn

迈克菲产品参考指南（2020 版）

McAfee Confidential

迈克菲重点安全解决方案

咨询订购：400-010-8885、 Support@mcafees.com.cn



设备

- 可视化和情景控制
- 数据保护
- 威胁检测和响应

安全运营

- 平台级数据保护
- 平台级威胁检测和响应
- 自动化 & Orchestration (主动 / 被动)

云

- 在私有云、混合云、公有云环境下的可视化和情景控制
- 数据和实例保护
- 威胁检测和响应

迈克菲整合安全防御框架

由分析驱动的威胁和数据防御

咨询订购：400-010-8885、 Support@mcafees.com.cn

协同
覆盖威胁防御生命周期

自动化
解决方案工作流

集成
核心技术和生态系统

产品参考卡

咨询订购：400-010-8885、 Support@mcafees.com.cn

设备	传统防护 + 机器学习 (ENS)	检测 & 响应 (EDR)	数据保护 & 加密 (DLP / MDE)	应用控制 (MAC/MCC)
安全运营	SOC 运营平台 (ESM)	沙箱 (ATD)	SOC Insight (Investigator)	SOC 服务 (FoundStone)
云	CASB (Skyhigh)	WEB安全防护 (MWG/SaaS)	云安全 (CWS)	网络安全 (NSP)

开放的平台	Open Management Platform	Threat Sharing (Open DXL)	Ecosystem (SIA)

端点安全产品 (Endpoint Security)

咨询订购：400-010-8885、 Support@mcafees.com.cn

1.1. 产品概述

1. 保护企业主机系统避免病毒，蠕虫，木马等各类恶意程序威胁。
2. ePO 终端系统安全套件提供集中的、简化的终端安全管理平台。
3. 将防病毒、防火墙、主机 IPS、WEB 管控无缝集成在一起。
4. 在传统防病毒技术的基础上，加入了智能的机器学习和应用容器等全新技术，从而更有效地应对勒索软件这一类的高级恶意代码。

1.2. 询问客户的问题

1. 贵公司是否感染过勒索软件？
2. 您是否了解端点安全市场已经出现了很多最新的技术？
3. 您是否了解安全需要通过不断进行升级，才能更有效地应对最新发生的威胁？

2. 产品功能和优势

单一控制台，单一代理	• ePO 集中管理平台，部署和维护容易，提高效率。减少部署成本，全方位覆盖 Windows、OS X、Linux 等各种平台
全新的安全防护技术	• 智能机器学习和应用容器技术 • 有效检测防御勒索病毒等高级恶意代码
集成性	• 整合 DXL 架构体系， 可以实现与 NSP、ATD、MWG、SIEM 全方位的联动
实时端点检测和响应	• 实时查找用户系统中的文件代码，快速消除恶意威胁 • 持续监控系统中的事件或状态变化，并根据规则作出响应保护系统

3. 成功案例

行业	客户
金融	中国银行、建设银行、浦发银行 平安保险、前海人寿、泰康人寿 上海证交所、国泰君安，中信建投，中泰证券
制造业	华为、中兴通讯、歌尔、浙江大华、中车集团、青岛四方、东风商用车、海信
互联网	携程、网易、大疆、摩拜
其它	万科、万达、顺丰、世茂集团、香格里拉、安踏

4. 主要型号

产品	功能型号	说明
ETX	ENS（Windows、Mac、Linux）、设备控制、邮件服务器安全、老版本 VSE、防火墙、WEB 管控、自适应威胁防御（机器学习、容器防御零日威胁、勒索病毒等），ePO 管理平台	按端点数量计价
CTX-C	ENS（Windows、Mac、Linux）、自适应威胁防御（机器学习、容器防御零日威胁、勒索病毒等）、设备控制、邮件服务器安全、老版本 VSE、防火墙、WEB 管控、应用白名单Application Control、ePO 管理平台	按端点数量计价
CTXU-C	原EPS或ETP升级至CTX-C	按端点数量计价

云/虚拟化安全产品 (CWS)

咨询订购：400-010-8885、 Support@mcafees.com.cn

1.1. 产品概述

1. 保护企业虚拟服务器、虚拟桌面避免病毒，蠕虫，木马等各类恶意程序威胁。
2. 有效降低防病毒系统对于虚拟化环境的资源消耗。
3. 监控发现虚拟化环境中的工作载荷

1.2. 询问客户的问题

1. 贵公司是否部署有服务器虚拟化或桌面虚拟化的环境？
2. 虚拟化环境中部署的是传统防病毒吗？
3. 是否存在虚拟化环境下资源消耗大、用户体验差的问题？

3. 成功案例

行业	客户	部署环境
金融	中国银行、建设银行、浦发银行、中国平安	桌面虚拟化 服务器虚拟化
制造业	华为、天马微电子、中车青岛四方、东方雷诺	桌面虚拟化 服务器虚拟化
零售业	百安居、百威	桌面虚拟化 服务器虚拟化

2. 产品功能和优势

统一管理平台 ePO	• 虚拟化、终端、服务器、Linux、MAC、存储等所有防病毒系统都由 ePO 统一管理、统一升级
VMware 合作伙伴	• 提供无代理解决方案，支持最新NSX架构
多平台支持	• 同时支持 HyperV、Xen、KVM、Huawei Fusionsphere 等各种虚拟化平台，以及AWS、Azure云平台
集成性	• 整合 DXL 架构体系， 可以实现与 TIE、ATD 整合，提升威胁检测能力

可视化监控虚拟化环境，确保工作载荷处于保护状态

4. 主要型号

产品	功能型号	说明
CXB-C	Cloud Workload Security for hybrid cloud, ENS for Server, MOVE Agentless, MOVE Multi-Platform, VSE/VES for Linux, ePO 管理平台	按OS数量
CXE-C	loud Workload Security for hybrid cloud, ENS for Server,ATP模块,TIE, MOVE Agentless, MOVE Multi-Platform, VSE/VES for Linux, ePO 管理平台	按OS数量
CXA-C	loud Workload Security for hybrid cloud, ENS for Server,ATP模块,TIE, MOVE Agentless, MOVE Multi-Platform, VSE/VES for Linux,Network Visibility, Application Control, Change Control, ePO 管理平台	按OS数量
MOV	ENS for Server(Threat Prevention, Firewall, Web Control), VSE, MOVE Agentless, MOVE Multi-Platform, Connectors for cloud, ePO管理平台	按OS数量
MOD-C	ENS for VDI(Threat Prevention, Firewall, Web Control), VSE, MOVE Agentless, MOVE Multi-Platform, Connectors for cloud, ePO管理平台	按OS数量

数据防泄漏 (DLP)

咨询订购：400-010-8885、 Support@mcafees.com.cn

1.1. 产品概述

1. 在企业网络出口监控、阻断（邮件或 WEB）敏感数据的外泄
2. 在办公室、路上、家中防止终端上各种可能的数据外泄
3. 对 Windows、Mac 系统的磁盘加密和管理，防止设备丢失导致的数据外泄
4. 对文件或介质进行加密处理，在内网信息交换过程中提供数据保护

1.2. 询问客户的问题

1. 贵公司终端上是否可能接触到敏感的数据，如设计图纸、源代码、项目计划、客户信息、业务信息？
2. 这些终端是否部署有保护这些敏感数据的技术手段？
3. 如果敏感数据被加密，在业务上是否需要解密数据后发送给合作伙伴或客户？
4. 如何实现敏感数据传输过程中的有效监控和审计？

3. 成功案例

行业	客户	部署环境
汽车制造	一汽大众、上汽、通用汽车、东风汽车、广汽、联合汽车电子、小糸车灯、中车株洲/青岛电动机车	网络 DLP 终端 DLP
医药	拜尔中国、先锋药业、迈瑞	网络 DLP/终端 DLP
金融	平安集团、银联、诺亚财富	终端 DLP
其它	玫琳凯、阿里巴巴、唯品会、上海文广传媒	DLP、加密

2. 产品功能和优势

1. 端点 DLP、网络 DLP、加密技术结合的整体数据保护解决方案
2. 端点 DLP 提供独特的标签技术，有效保护设计图纸、工艺流程、源代码等非结构数据
3. 在 Office 软件中嵌入数据分类按钮，提示用户对数据分类，从而达到用户教育的目的
4. 网络 DLP 缺省提供全捕获技术，满足审计监控的管理要求
5. 支持OCR技术对图片内容进行识别
6. 加密和 DLP 在 Gartner 评估中位于领导者象限
7. ePO 统一管理，降低端点资源消耗，提升管理运维效率
8. 整合 DXL 架构体系，控制未知威胁程序对重要数据的访问

4. 主要型号

产品	功能型号	说明
TDL	网络监控 DLP、网络阻断 DLP、网络发现 DLP、端点 DLP、 网络DLP(Mobile), ePO 管理平台	根据用户数计价
OCR	网络DLP识别图片中的内容（TDL附加模块）	根据用户数计价
CDB	磁盘加密、MS BitLocker & Apple FileVault加密管理、文件 & 移动介质加密、ePO	根据用户数计价
CDA	端点DLP、外设控制、磁盘加密、MS BitLocker & Apple FileVault加密管理、文件 & 移动介质加密、ePO	根据用户数计价
6600DLP-A	网络 DLP 硬件，用于网络监控和网络阻断模块、型号 6600	硬件（需购买软件许可）
CSADLP-A	满足Capture功能，提供16TB存储	硬件（搭配6600设备）

网络安全平台 (NSP)

咨询订购：400-010-8885、 Support@mcafees.com.cn

1.1. 产品概述

1. 保护重要业务系统，阻挡扫描探测、网络入侵、以及分布式拒绝服务等各种攻击。
2. 检测并拦截网络病毒、蠕虫、木马、僵尸网络威胁，并且能够和 APT 防范设备联动对高级恶意代码进行防范。
3. 网络区域分段保护，消除互联网和第三方网络安全威胁。
4. 私有云环境中网络威胁检测过滤。

1.2. 询问客户的问题

1. 重要业务系统和网络基础设施是如何保护的？
2. 网络安全区域是如何划分和保护的？
3. 如何对网络病毒和蠕虫进行检测和隔离的？
4. 私有云或虚拟化平台中的网络威胁如何检测过滤的？

3. 成功案例

行业	客户	部署环境
金融	太平洋保险、浦发银行、交通银行、中国银联、兴业银行、太平保险、上海证交所，建设银行，邮储银行	数据中心，广域网边界，分支机构、内部办公网
制造业	一汽大众、通用汽车、上海贝尔	数据中心 ERP 系统入侵防护
电信	河北联通、中国移动	BOSS 系统 骨干网网络恶意代码检测
其它	联想、华为、阿里巴巴、携程、玫琳凯、迪士尼	数据中心和网络边界安全防护

2. 产品功能和优势

性能卓越	• 稳定性达到 99.999%，可信赖电信级网络产品 • 单台处理能力可达 40Gbps
高级全面防护能力	• 内置多种不需要依赖特征库的威胁识别技术，无与伦比的主动防御机制
集成性和易用性	• 整合DXL架构体系，可与端点、网关、安全管理系统实现威胁情报共享，以及策略自适应调整 • 管理维护简易，大大提升了管理员的工作效率
全球市场份额第一，多年来位于 Gartner 领导者象限	
提供虚拟 IPS 方案，适用于 SDDC 数据中心的需求(支持Vmware、AWS、Azure、OCI等环境)	

4. 主要型号

企业规模	型号	处理能力
小企业	NS3100/NS3200/NS3500 NS5100/NS5200	100M/200M 600M/1G
中型企业	NS7150/NS7250/NS7350	1.5G/3G/5G
大型企业	NS9100/NS9200/NS9300 NS9500	10G/20G/40G 10G/20G/30G
出站SSL解密	IPS NS92-OSSL/IPS NS91-OSSL IPS NS73-OSSL/IPS NS72-OSSL	订阅许可，配合NSP设备
私有云或虚拟化	IPS-VM1000-CLD IPS-VM1000-CLD-SUB	200M/500M/1G 1G（订阅许可）
Oracle云平台	IPS VNSP OCI 25/100/250/500/1000	基于Oracle云上的主机数量

Web 安全网关 (Web Gateway)

咨询订购：400-010-8885、 Support@mcafees.com.cn

1.1. 产品概述

1. 针对互联网访问提供安全控制和专业网址过滤功能
2. Web 网关防病毒，防范恶意代码注入、木马、钓鱼攻击，检测僵尸网络
3. 集成行业领先的 DLP 技术，防护用户在上网过程中导致的企业敏感数据丢失
4. 反向代理保护企业互联网区域的WEB服务器

1.2. 询问客户的问题

1. 您知道勒索软件一定需要连接互联网才能感染加密数据吗？
2. 贵公司是否需要对内部感染木马、肉鸡的终端进行检查、监控？
3. 您知道上网行为管理类产品根本就不是用于恶意代码过滤的吗？
4. 您知道绝大部分对安全重视的企业，在网络基础架构的规划上，防火墙和用户上网安全网关都是必选项吗？

3. 成功案例

行业	客户
金融	建设银行、中国银行、光大银行 太平洋保险、平安保险、中国人寿、瑞士银行
制造业	华为、联想、东软、阿尔卡特、拜尔中国、海信
政府	天津滨海新区政府
媒体	天津电视台

2. 产品功能和优势

1. 目前业界最高安全等级的 WEB 网关防护产品，在第三方权威机构 AV-Test 评测的 WEB 网关安全产品排名第一
2. 与端点产品充分整合，无论是在办公室、家、出差都可以提供 7x24 小时不间断地 WEB 安全保护
3. 集成 ATD 沙箱技术，增强高级恶意代码的检测和阻断能力
4. 整合 DXL 架构体系，可与端点、网络、安全管理系统实现威胁情报共享，以及策略自适应调整
5. 详尽的用户访问网站的审计报表功能

4. 主要型号

产品	功能型号	说明
WG4500-D	100-1500 用户	小企业/分支机机构
WG5000-D	1500-3000 用户	中型企业
WG5500-D	3000-5000 用户 多台 HA/LB 支持更多用户	大型企业
WG4500-D-RP WG5000-D-RP WG5500-D-RP	反向代理网关	保护 WEB 服务器
WSG	WEB分类、内容过滤、URL 过滤、代理缓存、防病毒、SSL 扫描、WEB 报表	永久软件许可 根据用户数计算
WPS	WEB分类、内容过滤、URL 过滤、代理缓存、防病毒、GAM引擎、SSL 扫描、WEB报表、WEB Cloud服务	订阅软件许可 根据用户数计算
WGI	ICAP部署模式，防病毒过滤	永久软件许可 根据实例数量

检测与响应 (EDR)

咨询订购：400-010-8885、 Support@mcafees.com.cn

1.1. 产品概述

1. 在端点上持续监控关键事件和状态的变化
2. 收集并展现所有的文件信息，包括可执行和静止的
3. 自动化的响应规则来应对高级威胁
4. 帮助管理员近乎实时地对设备进行检测和修复

1.2. 询问客户的问题

1. 贵公司感染了高级威胁（勒索软件、APT、零日攻击）如何进行修复？
2. 贵公司感染了高级威胁后，如何在数千或数万台设备上检查是否存在潜在的安全隐患？
3. 贵公司是否需要对设备的安全状态进行持续的可视化监控，如进程、注册表、网络通信？
4. 贵公司是否觉得有必要将整合SOC平台实现自动化的安全运维？

2. 产品功能和优势

1. 与端点防病毒无缝集成，并由EPO统一管理。
2. 实时监控进程、文件、注册表、网络通信的状态，发现高级威胁自我删除进行隐藏的行为。
3. 整合 DXL 架构体系，配合SOC平台，可以实现自动化的响应处理，大大提升安全运维的时效性。

3. 成功案例

行业	客户
金融	ING, City Bank, Bangkok Bank, Swedbank，平安集团
制造业	HollyFrontier, GM, Fujisu
其它	顺丰, MGM, Hertz

4. 主要型号

产品	功能型号	说明
EDR1	包括Active Response、TIE Server、ENS Adaptive Threat Protection（DAC & Real Protect）、DXL、EPO管理服务器	按端点数量计价（需购买ETP）
EDR2	包括Active Response、TIE Server、DXL、EPO管理服务器	按端点数量计价（仅针对CTX-C用户）

威胁情报交换系统 (TIE)

咨询订购：400-010-8885、 Support@mcafees.com.cn

1.1. 产品概述

1. 结合全球威胁信息和本地收集的威胁情报，建立每个企业所特有的威胁情报中心，通过此中心实现对高级威胁（APT、零日攻击、高级恶意代码）的深层次防御
2. 将终端、网关、网络和数据中心的安全系统整合起来，实现威胁情报的即时共享，以及自适应的检测和响应
3. 基于迈克菲的安全联盟，整合更多的第三方系统

1.2. 询问客户的问题

1. 针对高级威胁（APT、零日攻击、高级恶意代码）您是否感觉无论是黑名单还是白名单技术都难以防范？
2. 您是否觉得需要对于在企业网络中使用的文件建立一个自己的情报分析中心？
3. 您是否觉得有必要将威胁情报在不同系统中实现信息交换共享？

2. 产品功能和优势

1. 即时监控企业内部是否存在高级针对性攻击
2. 将本地威胁情报和全球情报数据源提炼整合
3. 目前业界唯一可实现终端、网关、网络和数据中心安全系统实时共享威胁情报的解决方案
4. 可从检测、防御、修复三个不同安全防护的角度协调保护用户环境，并做出自适应的调整
5. 通过 DXL 数据交换架构，可以实现与不同厂商产品的威胁情报共享

3. 成功案例

行业	客户
制造业	华为、歌尔、阿尔卡特、努比亚、蔚来汽车、富士通
金融	平安集团、中信银行国际、建行亚洲、普华永道
电信	香港电讯、台湾移动、Telstra
其他	顺丰

4. 主要型号

产品	功能型号	说明
TIE	TIE、ePO 管理平台	按端点数量计价

应用程序白名单 (Application Control)

咨询订购：400-010-8885、 Support@mcafees.com.cn

1.1. 产品概述

1. 对计算机和嵌入式设备提供基于白名单技术的安全保护，无须依赖于特征库更新
2. 对列入白名单中的应用程序进行安全保护，防护这些程序被攻击
3. 能够保护服务器、办公计算机、嵌入式设备，包括 ATM、POS、自助体验设备、SCADA 等
4. 能够对厂商已经不提供安全补丁的老旧操作系统，比如 Windows NT、2000、XP 等提供安全保护

1.2. 询问客户的问题

1. 您如何保护您的服务器？如果没有安全补丁或者不能使用安全补丁的情况下，如何保护您的服务器或者计算机的安全？
2. 您的嵌入式设备（ ATM、POS、自助体验设备、SCADA 等）有安全保护吗？
3. 您是否担心在设备上安装安全软件会影响性能和系统正常使用？

3. 成功案例

行业	客户
金融	中国银行、汇丰银行、中信银行国际
制造业	通用汽车、华为、DELL、NCR、联发科、大众、中石化、霍尼韦尔、西门子
其他	WebEx、电讯盈科、迪斯尼、屈臣氏、天虹商场

2. 产品功能和优势

1. 支持多种主流操作系统，包括 Windows 各类操作系统和 Linux
2. 支持动态白名单技术，可以基于自学习、更新程序设定、可信目录、可信证书等机制大大减轻管理员负担
3. 支持用户自批准和管理员审计功能，方便在办公终端上部署
4. 具有内存保护技术，防止列入白名单的程序被入侵利用
5. 具有程序库功能，能够把文件分为黑、白、灰三类，并且支持全球威胁智能感知 (GTI) 技术，能够智能识别被误列入白名单中的恶意程序
6. 防范通过利用Powershell等工具产生的无文件恶意代码
7. 计算机资源消耗很低，不影响系统正常运行。CPU 1%，内存 8-16M
8. 整合 DXL 架构体系，可与端点、网络、网关、安全管理系统实现威胁情报共享，以及策略自适应调整

4. 主要模块

套件	功能型号	说明
ACD	Application Control for PC，适用于桌面计算机保护	按端点数量计价
ICD	McAfee Integrity Control for Fixed Function Devices，包含了 Application Control 和 Change Control 模块，适用于嵌入式设备保护（包括 ATM、POC、自助设备、SCADA）	按设备数量计价
ACS	Application Control for Server，适用于老旧服务器的保护（无法安装防病毒）	按服务器数量计价

高级威胁防御设备 (ATD)

咨询订购：400-010-8885、 Support@mcafees.com.cn

1.1. 产品概述

1. 采用沙箱 (Sandbox) 技术，发现防病毒基于黑名单技术无法识别的高级恶意代码和目标型攻击
2. 对通过网络、电子邮件、Web、终端等多种渠道传播和感染的恶意代码进行检测和拦截
3. 支持对常用 Windows 操作系统和 Android 平台的病毒文件分析
4. 提供硬件和虚拟化两种部署方式

1.2. 询问客户的问题

1. 贵公司是否感染过勒索软件？
2. 贵公司是否了解传统防病毒技术对于高级威胁（勒索软件、APT、零日攻击）的防护效果不佳？
3. 贵公司是否觉得有必要将沙箱技术与现有部署的端点、网络、网关等产品整合部署？

3. 成功案例

行业	客户
金融	太平保险、平安集团、中信银行国际、建行亚洲、台湾商业银行、台湾银行、台湾证交所
制造业	华为、阿尔卡特、努比亚、和舰科技、NCR、UMC、蔚来汽车
其它	百度、香港电讯、中信建投、Wipro、Telstra、Intel、CA

2. 产品功能和优势

1. 在动态沙箱分析 (Sandbox) 前、通过黑白名单、云 GTI 检测、病毒检测、网关恶意代码检测、Yara 规则等检测技术，大大提升沙盒的处理分析效率。
2. 通过深度神经网络（DNN）技术实现机器学习，提高对未知威胁的检测能力。
3. 通过文件的静态代码分析技术，即脱壳和反汇编，发现试图绕过沙箱技术的高级恶意代码。
4. 部署方式灵活，可与端点防病毒、网络 IPS、WEB 网关、第三方邮件网关、防火墙、自定义接口进行整合，而且单台设备可以同时支持与不同系统的集成，节省部署成本。
5. 支持集群，可以按需进行扩展。
6. 整合 DXL 架构体系，不单单做检测，还可以实现自动化的响应处理，大大提升安全运维的时效性。

4. 主要型号

企业规模	型号	处理能力
中小企业	ATD-VM1008	提供8个虚机的分析实例（可堆叠）
中大型企业	ATD-3100	硬件，提供30个虚机的分析实例
大型企业	ATD-6100	硬件，提供60个虚机的分析实例
邮件用户	ATD-VM1008-EMAIL	虚机实例，基于用户邮箱数量计价
MWG用户	VATD WSG	无限虚机实例，基于MWG用户计价
NSP用户	VATD IPS NSxx00	无限虚机实例，基于NSP型号数量计价
CTX端点用户	ATD-VM1008-EP	虚机实例，基于端点数量计价

安全日志和事件管理 (SIEM)

咨询订购：400-010-8885、 Support@mcafees.com.cn

1.1. 产品概述

1. 实时收集多种、海量的日志和事件信息，并对这些海量信息进行关联分析，发现潜在安全风险
2. 将对外界信息（威胁数据、信誉数据和漏洞资讯）的实时了解与对企业内部的系统、数据和活动的实时信息联系起来
3. 支持对数据库交易和应用层的分析和挖掘

1.2. 询问客户的问题

1. 贵公司由于合规性要求（ISO、等保、监管机构），是否存在日志集中存储、实时查询方面的需求？
2. 面对各种不同厂商的系统设备以及海量的日志，是否需要进行标准化、智能的分析，帮助管理员快速发现正在发生的安全威胁？
3. 面对海量日志，是否需要实时仪表板展现和周期性报表？
4. 如何管理、分析和利用安全威胁情报？

3. 成功案例

行业	客户
制造业	上海大众、联想、阿尔卡特、联合汽车电子、HTC
金融	太平洋保险、兴业银行、华一银行、信诚人寿
电信	海南移动、SK 电信
其它	万达、德勤、东方航空、艾默生、深圳地铁

2. 产品功能和优势

1. 业界最快速的 SIEM，支持数十亿信息记录的快速关联和查询。单个 ESM 每秒钟可以支持 400000 事件
2. 和全球威胁智能感知系统 (GTI) 整合，快速识别潜在安全风险
3. 整合 DXL 架构体系，与网络安全设备 (NSP) 联动实现自动化的威胁阻断隔离，与端点安全管理台 (ePO) 集成实现端点的自动化修复
4. 内置 200 多种开箱即用的关联分析规则，管理员只需简单激活策略，就可以实时监控发现网络中发生的安全威胁。内置UBA功能。
5. 能够支持多种格式和类型的威胁情报导入、管理和自动化关联分析。
6. 预置数百个合规报表模板，包括 ISO 270001、PCI DSS、HIPAA、NERC-CIP、FISMA、GLBA、SOX 等
7. 管理员界面简单易用，提升运维效率

4. 主要型号

产品	功能型号	说明
ESM-ELM-ERC-5700 ESM-ELM-ERC-6050 ESM-ELM-ERC-VM	中小企业	包括 ESM、ELM、ERC 和关联分析功能模块 原始日志存储需要外置存储设备
ESM-VM ETM-5700 ETM-6050	中小企业	分布式架构 需另配置 ERC、ELM、ACE 模块
ESM-VM ESM-X7	大型企业	分布式架构 需另配置 ERC、ELM、ACE 模块
ETM-X9 ETM-X11	超大型企业或 SaaS 架构	分布式架构 需另配置 ERC、ELM、ACE 模块

关于我们

咨询订购：400-010-8885、 Support@mcafees.com.cn

迈克菲是全球领先的独立网络安全公司之一。秉承“联合就是力量”的精神，迈克菲致力于创建面向企业和个人用户的安全解决方案，使我们的世界更加安全。迈克菲的解决方案可与其它公司的产品协同工作，为企业提供真正集成的网络安全环境，使得威胁的防护、检测和修正能够同时执行且相互协作。通过保护个人用户的所有设备，迈克菲为他们提供安全的数字生活，无论身处何处。通过与其它安全厂商合作，迈克菲致力于联合整个安全行业的力量打击网络犯罪，保护我们数字世界的安全。

- 为90%的全球财富 100 强 企业提供保护
- 为 82%的全球财富 500 强企业提供保护
- 为 62%的全球 2000 强企业提供保护
- 为82%的全球最大的银行 提供保护
- 为 74% 的全球500强零售商提供保护

企业客户销售热线

400 010 8885 或 800 810 6669

咨询订购：400-010-8885、 Support@mcafees.com.cn