“思科AMP帮助企业构建高级恶意代码防护与响应体系”在线研讨会-精彩问答

序号	问题	回答
1	AMP这个解决方案需要购买一整套的沙盒、NGFW、WSA、ESA等配合使用吗?还是单独使用只是功能等区别?	AMP是一套覆盖网络边界、内容和终端的解决方案，用户可以选择单独在NGFW、WSA或者ESA上启用AMP的功能，AMP的端点解决方案和沙箱可以独立运行，沙箱可以采用公有云或者专用设备。
2	加入AMP防护体系以后，会不会让公司内部员工感觉上网会变慢?因为多了很多检测和过滤?	ESA邮件网关启用AMP，可以对恶意文件进行检测，邮件可以设定暂时隔离，等待检测结果出来后，选择邮件阻断或者放行，也可以选择检测的同时放行。网络边界NGFW / NGIPS启用AMP后，检测都是实时的，不会对上网有任何影响。端点AMP占用系统资源非常少，不会影响终端的运行。
3	请问IoC是什么信息?	IOC是Indicator of Compromise的缩写，就是用来判读恶意程序活动的指标和征兆
4	AMP的架构技术抓包分解吗?	AMP的架构不依赖抓包技术，对于文件的提取是在NGFW / NGIPS / ESA / WSA / AMP4E上进行的。
5	AMP 可以独立部署么?还是要整合其他安全平台使用才能发挥作用?	AMP是一套覆盖网络边界、内容和终端的解决方案，用户可以选择单独在NGFW / NGIPS / WSA / ESA启用AMP功能，用户也可以独立购买终端的AMP和沙箱设备。
6	AMP for Endpoint 需要搭配其它思科硬體設備?	AMP4E如果采用公有云管理，不需要任何其它设备，如果想部署私有云，需要搭建一个管理服务器和一台沙箱设备。
7	终端能够独立安装Endpoint来做一些病毒的防护吗?还是需要endpoint与AMP或FMC进行联动?	AMP的终端解决方案可以独立运行，内嵌了高级恶意代码检测和病毒引擎，可以检测病毒和高级恶意代码防护，不需要和FMC联动。如果防火墙启用了AMP，FMC也可以和AMP4E联动，可以把网络边界的发现和端点的发现集成在一起进行联防联动。
8	Endpoint能独立运行在终端上做病毒防护吗?	可以，AMP4E是独立的系统，可以进行高级恶意代码检测、防护和病毒防护。
9	AMP 部署在网络什么位置，需要专门的服务器吗，license怎么算的?	AMP可以采用公有云，也可以采用私有云，私有云的话需要安装服务器和沙箱组件，License可以在防火墙、邮件网关上启用AMP，端点License根据终端数量计算。

10	amp端点客户端怎么卖的。按照终端数吗 最低多少端点起卖?谢谢。	AMP端点按照客户端数量进行计算，数量用户可以自己选择。
11	ESA / WSA 上是否可以实现威胁回溯的功能?	ESA / WSA上启用AMP后，可以实现威胁回溯，可以追踪每个恶意程序的执行过程和风险级别。
12	原本安全附件被更新判定为恶意时是否会通知管理员?	原来的附件文件，经过AMP分析后确认为恶意的话， 一旦该文件再出现传播行为，就会被阻断，同时通知管理员。
13	对于网站下载这种方式，沙箱需要运行时间，有些恶意程序会直接进入内网，对于已经感染的内网主机，AMP方案除了上报事件还有什么解决方法?	网站下载了未知威胁文件，会发送到沙箱运行，同时文件会进入内网，AMP会记录恶意文件进入内网的传播路径，沙箱计算确认为恶意文件后，会同时更新到所有的解决方案，包括边界设备和终端，此时该文件如果再出现传播行为，会被阻断并上报。另外，AMP的端点检测引擎，除了使用沙箱外，可以对恶意文件本身进行病毒分析、机器学习和IOC检测，可以拦截恶意程序。
14	有没有测试过，对数据的延迟有多大?	这是一个复杂的问题，网络边界AMP没有延迟，邮件AMP根据策略可以设定邮件隔离或放行，端点轻量级运行，系统影响很小。
15	1、对于O365云端的邮件如何与AMP联动? 2、触发型的木马病毒如何沙箱? 3、进入沙箱的过程，用户端会有延迟吗? 4、U盘-PC-FTP的过程，终端会有防护吗?	1.一定要使用了ESA邮件网关，或者云端的邮件网关，才能和AMP联动 2.木马文件本身第一次传入的时候，可以发送到沙箱，在木马触发交互过程中，如果有payload文件的下载过程，都可以发送到沙箱，沙箱的运行用户可干预。 3.边界AMP不会有任何影响，邮件AMP可根据设定的邮件隔离或放行策略选择性隔离，端点AMP不会有延迟 4.端点AMP可以防护通过U盘拷贝恶意文件，可以监控和防护通过FTP等网络行为进行恶意代码的传输
16	Hash威胁库是不是业界首创的?	AMP的Hash库并非首创，但是是业界最大的库之一，和Talos保持数据同步。
17	AMP是一个体系还是一套设备?	参考以上回答，AMP是一套解决方案，可以和思科的边界安全设备、邮件网关、WEB网关结合，同时覆盖终端的高级恶意代码防护。
18	文件（比如邮件附件）是加密的，AMP可以检测吗?	加密文件可以被识别出为加密内容，但无法检测。

19	沙箱會有誤判機率嗎?	所有沙箱都会有，AMP的沙箱的判定过程是一个多钟方式关联和结合分析过程，有800多个IOC进行检测，采用风险得分机制，95分以上判定为恶意，其它分数用户可定义。
20	AMP和沙盒运算是否都是在云上进行的?不在本地运行?	AMP和沙盒有公有云，也有本地的私有云，用户可以搭建自己的本地系统。
21	AMP架构在非COSCO硬件上能实现吗?	AMP的端点解决方案和沙箱都可以在非思科换进行下独立运行，边界、邮件和WEB需要和思科设备集成。
22	现在越来越多的企业使用O365这类SAAS的邮件系统，AMP在这方面是如何支持的?因为邮件网关已经不在企业内部了?	AMP的邮件附件检测需要和ESA邮件网关或思科云端邮件网关集成，如果用户使用思科的云端邮件网关，可以实现AMP的集成。
23	AMP是一个独立产品，还是说分散在cisco各类安全产品中的一个特性，只需激活就好?	参考以上回答，AMP是一套解决方案，边界安全设备、邮件网关、WEB网关需要激活AMP功能，终端防护方案和沙箱可以独立运行。
24	预防性防护的机制有较强的地方吗?	AMP拥有全球共享文件信誉云，全球情报同步，AMP会在管理平台上预警当前全球发现的最新威胁和漏洞，建议用户进行防护，提高预警能力。
25	CISCO的IPS和IDS与AMP功能上的区别?	IPS / IDS是根据签名对数据包进行检测的机制，AMP是对传输的文件本身进行分析，判断是恶意文件还是安全的文件。
26	AMP感觉像是集中运行在网络内部的，只不过他可以控制各种边界硬件产品，如IPS之类, 和网络杀毒软件，如趋势类似。	AMP不同于网络防病毒，更侧重于对于高级恶意代码的检测、防护和回溯，所谓高级恶意代码，就是传统防病毒无法及时检测的恶意程序，特点是变种快、利用新漏洞、采用非病毒特征的脚本代码等方式，如果防病毒能检测到高级恶意代码，就不会出现那么多勒索软件安全事故了。
27	AMP会不会泄露个人文档?	如果企业关心信息安全，可以采用本地的AMP私有云系统进行管理和运行。
28	AMP对pc、服务器和网络的性能有多大影响?即AMP占用的资源是怎样的?	AMP不同于传统防病毒，采用Hash查询和沙箱动态分析机制，对系统资源占用很少，性能影响很低。

29	进行持续性回溯，是对所有文件都追踪?若是，会占用多少系统资源?	回溯分为两种：文件回溯和设备回溯，文件回溯可以判断一个恶意文件或者未知文件的传播途径，安全的文件并不进行记录。设备回溯可以分析和监控设备的进程调用关系，系统占用资源很少。
30	若要建2个私有云，这2个云要多大才能发挥效果?	文件信誉系统会从云端同步更新所有的Hash库，放在本地进行分析，本地发现的文件都可以到文件信誉系统进行分析，沙箱私有云可以部署一台专用的沙箱设备，设备分为高端和低端型号，满足不同文件数量的沙箱分析。
31	上网速度不会受影响?上网的文件存取不会进入沙箱?	上网速度不会受到影响，上网下载的文件如果是未知的威胁文件，会发送到沙箱。