FUNCIONALIDADES	CYTTEK ATM SECURITY	MCAFFE	GMV	SYMANTEC	TREND MICRO	BIT 9
PROTECCIÓN CONTRA EL FUNCIONAMIENTO NO AUTORIZADO DE SOFTWARE						
LA PROTECCIÓN CONTRA AMENAZAS DE DÍA CERO CONTRA ATMS		1	1	1		
TECNOLOGÍA DE LISTA BLANCA						
DETECCIÓN CON FALSO POSITIVOS						
PROTECCIÓN CONTRA EL USO NO AUTORIZADO DE LIBRERÍAS (DLLS) Y UNIDADES DE ALMACENAMIENTO						5
PROTECCIÓN CONTRA EL USO NO AUTORIZADO DE DISPOSITIVOS PERIFÉRICOS	3	3				6
PROTECCIÓN CONTRA EL ACCESO NO AUTORIZADO ARCHIVOS Y CARPETAS EN EL CAJERO AUTOMÁTICO						
PROTECCIÓN CONTRA EL FUNCIONAMIENTO NO AUTORIZADO EL CÓDIGO DE JAVA	8					
PROTECCIÓN CONTRA EL ACCESO NO AUTORIZADO A REGISTRO DE WINDOWS						
VERIFICACIÓN DE LA INTEGRIDAD DE LOS ARCHIVOS EJECUTABLES, LAS BIBLIOTECAS Y LOS CONTROLADORES						
VERIFICACIÓN DE LA INTEGRIDAD DE TODOS LOS ARCHIVOS EN EL CAJERO AUTOMÁTICO						
CORTAFUEGOS INCORPORADO PARA CONTROL DE COMUNICACIONES PARA CADA PROCESO						
CONTROL DEL TECLADO						
POLÍTICAS UNIFICADAS PARA FIREWALL Y APLICACIONES CONTROLADORES						
CONTROL DE ACCESO ADAPTABLE EN FUNCIÓN DE EL USO						
EL CONTROL DE LOS USUARIOS EN GENERAL Y CONTRASEÑAS DEBILES						
ELIMINACIÓN AVANZADA DE ROOTKITS				1		
MODO SOLO REGISTRO DE EVENTOS						
CIFRADO COMPLETO DEL DISCO						
DETECCIÓN DE ESCRITURA SOBRE DATA CARD TRACK 2						
COMUNICACIÓN CIFRADA ENTRE EL AGENTE Y EL SERVIDOR						
CONTROL DE EJECUCIÓN DE PROCESOS EN MEMORIA						
SSL/TLS CERTIFICATE PINNING WINDOWS CERTIFICATE MANAGER						
PROTECCIONES DE STRUCTURED EXCEPTION HANDLER OVERWRITE PROTECTION (SEHOP)						
IMPLEMENTACIÓN DE PROTECCIONES EN SOFTWARE COMPILADO DATA EXECUTION PREVENTION (DEP)						
IMPLEMENTACIÓN DE PROTECCIONES HEAPSPRAY ALLOCATIONS						
IMPLEMENTACIÓN DE PROTECCIONES MANDATORY ADDRESS SPACE LAYOUT RANDOMIZATION (ASLR)						
EXPORT ADDRESS TABLE ACCESS FILTERING (EAF) - WINDOWS API PROTECTION (KERNEL32.DLL, NTDLL.DLL OR KERNELBASE.DLL, ETC..)						
EXPORT ADDRESS TABLE ACCESS FILTERING PLUS (EAF+)						
VERIFICACIÓN DE CARGA DE LIBRERIAS DINAMICAS						
ATTACK SURFACE REDUCTION (ASR) - PREVENIR CARGA DE DLLS PARA APLICATIVOS DE TERCEROS						
SISTEMA DE GESTIÓN DE PUNTOS DE RESTAURACIÓN DE PRODUCCIÓN						
IDENTIFICACIÓN Y MONITORIZACIÓN DE APLICATIVOS DE TERCEROS CONFIGURADOS EN EL AUTO ARRANQUE DEL SISTEMA						
IMPLEMENTAR CONTRASEÑA DE BIOS DELL REMOTAMENTE						
XFS ERROR MONITOR PARA PROBASE/PROCASH, APTRA, AGILIS, DYNASTI JAM , KAL						
REPORTE DE TRANSACCIONES Y EFECTIVO EN LA RED DE ATM COMPLETA						
GESTION DE POLITICAS DE CONTROL DE REPOSICIÓN DE EFECTIVO						
HARDWARE SECURITY						
MONITORIZADOR DE ABERTURA DE BOVEDA O FASCIA						
MONITORIZADOR DE VIBRACIONES EN EL CAJERO						
CONECTOR PARA ANTI SKIMMERS DE TERCEROS						
MIDDLEWARE SECURITY						
PORT MIRRODING						
TRANSACTION MACHING						
IMPLEMENTACIÓN DE BLOQUEO DE PROCESOS DE DISPENSADO SIN AUTORIZACIÓN						
CAPACIDADES DE RESPUESTA A INCIDENTES Y EJECUCIÓN FORENSE REMOTA						
SISTEMA DE RESPUES A INCIDENTES REMOTO EN TIEMPO REAL						
INTERFAZ GRAFICA PARA LA GESTIÓN AVANZADA DE RESPUESTA A INCIDENTES						
MAS DE 90 MODULOS FORENSES PARA LA INVESTIGACIÓN DE DLLS, DRIVERS, PROCESOS MEMORIA, HISTORIAL DE TODO EL SISTEMA WINDOWS, LLAMADAS API WINDOWS, KERNEL PROCESSES , HOOKS , INVESTIGACIÓN Y DETECIÓN DE INCIDENCIAS AVANZADAS EN TIEMPO REAL						
POLÍTICAS DE SEGURIDAD						
CONTROL INTEGRAL DE LA PROTECCIÓN ATM A TRAVÉS DE LA POLÍTICA DE SEGURIDAD						
MÓDULO DE EDICIÓN DE DIRECTIVAS EMBEBIDO DESDE LA CONSOLA						
COMPATIBLE CON LA DEFINICIÓN AUTOMÁTICA DE LAS POLÍTICAS A TRAVÉS DE AUTOAPRENDIZAJE						
EXPORTACIÓN / IMPORTACIÓN DE LAS POLÍTICAS EN ARCHIVOS XML				1	1	1
GESTIÓN INTEGRAL DE LA VERSIÓN EL CONTROL Y LA CONFIGURACIÓN						
FIRMADO DE FICHEROS DE CONFIGURACIÓN				1	1	1
DESARROLLO DE POLITICAS CENTRALIZADAS						
ACTUALIZACIÓN DE POLÍTICAS “ON THE FLY”		1				
ACTUALIZACIÓN DE POLÍTICAS POR CONSOLA				1	1	1
RESPUESTA DE ALERTAS CON CAPACIDADES FORENSES						
MONITOREO Y AUDITORIA						
AUDITORÍA DEL FICHERO DE REGISTRO Y EVENTLOG WINDOWS				1	1	1
AUDITORÍA CENTRAL DEL REGISTRO DE WINDOWS						
CONTROL DE SEGURIDAD A TRAVEZ DE UN DASHBOARD						
ANÁLISIS DE TIEMPO REAL DE EVENTOS				1	1	
CONSULTA DE EVENTOS ANTERIORES						
REPORTES DE EVENTOS UNIFICADOS						
GESTIÓN BASADAS EN PERFILES						
SOPORTE NATIVO PARA INTEGRACIÓN CON OTRAS APLICACIONES				1	1	
EXTRACCIÓN DE JOURNAL XFS						
GESTION DEL AGENTE						
ACTUALIZACIÓN AUTOMÁTICAS		4		1		
SE REQUIERE DE SERVIDORES EXTERNOS PARA ACTUALIZACIÓN						
REGISTRO AUTOMÁTICO DE AGENTES A LA RED						
ACTIVACIÓN Y DESACTIVACIÓN DE AGENTES ATRAVES DE UN DASHBOARD						
AUTENTIFICACIÓN Y CIFRADO DE COMUNICACIONES ENTRE SERVIDOR Y AGENTE				2	2	1
NO REQUIERE DE CAMBIOS EN EL EQUIPO PARA SU FUNCIONAMIENTO						
OTRA FUNCIONALIDADES						
AGENTES PARA MULTIPLES PLATAFORMAS						
ALL IN ONE (A DIFERENCIA DE PAQUETE DE PRODUCTOS)						
AGENTES DISPONIBLES PARA WINDOWS NT (NT4.0)						
AGENTES PARA WINDOWS XP (SP1, SP2, SP3)						
AGENTES PARA WINDOWS 2000						
AGENTES PARA WINDOWS SERVER 2003, 2008, WINDOWS VISTA, WINDOWS7						
AGENTES PARA PLATAFORMAS UNIX-LIKE (LINUX, BSD, SOLARIS)						
MEMORIA RAM DE ATM (MÍNIMO REQUERIDO PARA LA INSTALACIÓN DEL AGENTE)	512MB*	256MB (1GB)	128MB	512MB (1GB RECOMENDADO)	256MB (1GB RECOMENDADO)	INFORMACION NO PROVEIDA
ESPACIO EN EL HARDDISK EN EL ATM (MÍNIMO REQUERIDO PARA LA INSTALACIÓN DEL AGENTE)	250MB	100MB	30MB	850MB	1	INFORMACION NO PROVEIDA
MODO DE SERVIDOR DE ALTA DISPONIBILIDAD (ACTIVO/ACTIVO Y ACTIVO/PASIVO)						
SERVIDOR CERTIFICADO PARA TRABAJAR CON BASE DE DATOS ORACLE						
SERVIDOR CERTIFICADO PARA TRABAJAR CON DB2 UDB Y BASE DE DATOS DB2 Z OS						
SERVIDOR CERTIFICADO PARA TRABAJAR CON SQL SERVER						7
SERVIDOR CERTIFICADO PARA TRABAJAR CON MYSQL						
SERVIDOR CERTIFICADO PARA TRABAJAR SOBRE BASES DE DATOS NO RELACIONALES						
SERVIDOR CERTIFICADO PARA TRABAJAR CON LINUX / AIX / SOLARIS						
LICENCIAS POR MANTENIMIENTO						
MECANISMO DE PROTECCIÓN CONTRA LA DESINSTALACIÓN DEL SOFTWARE						
MODO SIGILOSO PARA LA IDENTIFICACIÓN DE PATRONES DE ATAQUE						

(1) Con base en la información proporcionada en el sitio web del fabricante.
(2) La comunicación está cifrada, pero, clave de cifrado se define durante el tiempo de instalación y sigue siendo siempre la misma
(3) El producto se complementa con otros módulos de la suite de McAfee, como el control de dispositivos
(4) Requiere software adicional
(5) Se controla como cualquier otro archivo. No hay ninguna posibilidad de especificar los derechos procesos para cargar una DLL o un controlador.
(6) Sólo llaves USB y dispositivos de almacenamiento extraíbles
(7) Server sólo se puede implementar en Windows 2003 Server Estándar con SQL Server
(8) Si se tiene implementado protecciones de bajo nivel y de stack de memoria no se requere detección de falsos positivos
* Dependera de los recursos de aplicativos de terceros
**Los recuadros amarillos son configurados a medida del cliente el cual requieren cierta personalización unica para su seguridad