McAfee Application Data Monitor

Rileva le minacce nascoste con l'ispezione del livello applicativo.

L'appliance McAfee® Application Data Monitor porta la sicurezza e la conformità oltre i confini della gestione del log, monitorando tutto l'ambiente fino al livello dell'applicazione. Potrai ispezionare completamente i contenuti dell'applicazione per ottenere la visibilità più approfondita sul modo in cui viene utilizzata la rete.

L'appliance McAfee Application Data Monitor decodifica l'intera sessione di un'applicazione fino al livello 7, fornendo un'analisi completa di tutto, da protocolli soggiacenti e integrità delle sessioni ai contenuti dell'applicazione stessa (come il testo di un'email o i suoi allegati). Questo livello di dettaglio consente l'analisi accurata del reale uso dell'applicazione, permettendo anche di applicare relative policy di utilizzo e di rilevare il traffico maligno e occulto.

La profondità di questo tipo di ispezione è ideale per le esigenze di conformità in quanto tiene traccia di tutti gli usi dei dati sensibili in rete. Quando l'appliance McAfee Application Data Monitor rileva una violazione, conserva tutti i dettagli della sessione di quell'applicazione, per il loro utilizzo nella risposta agli eventi o per le esigenze di verifica della conformità.

Allo stesso tempo, l'appliance McAfee Application Data Monitor offre visibilità su quelle minacce che possono mascherarsi come applicazioni legittime:

- Minacce avanzate a livello dell'applicazione
- Furto o utilizzo non autorizzato di dati riservati
- Attacchi diretti o provenienti da "punti ciechi" della sicurezza
- Uso di codice legacy pericoloso
- Furto o abuso delle credenziali degli utenti
- Trasmissione di dati sensibili tramite qualsiasi applicazione
- Interruzione di processi aziendali

Perdita di dati e violazioni della conformità

L'appliance McAfee Application Data Monitor è in grado di rilevare il momento in cui le informazioni sensibili vengono trasmesse tramite allegati email, messaggi istantanei, trasferimenti di file, post HTTP o qualsiasi altra applicazione, avvisandoti immediatamente per poter mitigare le perdite.

Vantaggi principali

- Decodifica l'intera sessione, fino al livello 7, di centinaia di applicazioni
- Include regole di rilevamento incorporate per i dati regolamentati e sensibili
- Supporta regole e dizionari definibili dall'utente personalizzabili
- Genera un processo di verifica degli eventi delle applicazioni ai fini della conformità
- Opera in modo passivo per evitare interferenze con le applicazioni
- Si integra con McAfee Enterprise Security Manager per consentire la correlazione dei contenuti delle applicazioni con eventi e altri feed di dati
- Opzioni di distribuzione ibride flessibili includono appliance fisiche e virtuali

Puoi rilevare da subito i dati sensibili come informazioni di carte di credito e codici fiscali, oppure personalizzare le funzioni di McAfee Application Data Monitor definendo i tuoi dizionari di informazioni sensibili e riservate. L'appliance McAfee Application Data Monitor rileva questi tipi di dati sensibili, avvisa il personale idoneo e registra la trasgressione per mantenere una traccia al momento della verifica.

Individuazione documenti

L'appliance McAfee Application Data Monitor individua oltre 500 tipi di documenti mentre vengono scambiati sulla rete tramite email, chat, P2P, condivisione e altri mezzi. L'appliance McAfee Application Data Monitor individua i documenti indipendentemente dall'estensione per includere quelli che si camuffano con un'estensione diversa al fine di eludere i gateway di posta elettronica e i dispositivi di rilevamento e prevenzione delle intrusioni (IDS/IPS). Anche i documenti incorporati all'interno di altri, oltre ai file archiviati, compressi e codificati, vengono individuati con parametri quali il nome del file e l'operazione eseguita, in base ai quali viene determinata l'azione.

Le minacce a livello dell'applicazione

Le nuove e sofisticate minacce sfruttano le vulnerabilità presenti nelle comuni applicazioni aziendali per penetrare nella rete ed esportare i dati sensibili. Se queste minacce a livello dell'applicazione sono difficili da individuare con i tradizionali firewall, sistemi IDS e IPS, l'appliance McAfee Application Data Monitor è in grado di guardare all'intero contenuto di un'applicazione - compresi i protocolli soggiacenti - per rilevare payload nascosti, malware e addirittura canali di comunicazione occulti, come un eseguibile incorporato in un documento PDF.

Anomalie di protocollo

Rilevando le anomalie si possono identificare tempestivamente le minacce imminenti, ridurre i rischi e minimizzare le perdite. Mentre le alcune soluzioni di sicurezza tradizionali sono limitate all'analisi dei flussi di rete, l'appliance McAfee Application Data Monitor porta questo approccio a un livello superiore. Tale metodologia di rilevamento dei rischi più tempestiva guarda ben oltre i comportamenti in rete, per rilevare le anomalie all'interno di applicazioni e protocolli e offrire una protezione ancora più robusta.

Nessuna interferenza con le applicazioni

Dato che l'appliance McAfee Application Data Monitor opera su una porta SPAN, non interferisce né con le prestazioni delle applicazioni né con l'affidabilità e non introduce latenza.

Integrata con l'infrastruttura aziendale

Mentre la maggior parte delle soluzioni di monitoraggio della rete opera in modo isolato, l'appliance McAfee Application Data Monitor lavora di concerto con altri sistemi di protezione delle informazioni. Attraverso la soluzione McAfee Enterprise Security Manager, si collega al resto dell'infrastruttura di sicurezza per semplificare le operazioni di sicurezza, migliorare l'efficienza complessiva e ridurre i costi. È possibile integrare il rilevamento di perdite e frodi con analisi approfondite, ispezioni della rete, monitoraggio degli eventi del database e altre funzioni.

Oltre 500 applicazioni e protocolli supportati

- **Protocolli di rete di basso livello:** TCP/IP, UDP, RTP, RPC, SOCKS, DNS e altri
- **Email:** MAPI, NNTP, POP3, SMTP, Microsoft Exchange
- **Webmail:** posta elettronica AOL Webmail, Hotmail, Yahoo! Mail, Gmail, Facebook e MySpace
- **Messaggistica istantanea:** AOL, ICQ, Jabber, MSN, SIP e Yahoo
- **Protocolli di trasferimento file:** FTP, HTTP, SMB e SSL
- **Protocolli di compressione ed estrazione:** BASE64, GZIP, MIME, TAR, ZIP e altri
- **File di archivio:** archivi RAR, ZIP, BZIP, GZIP, Bin-hex e codificati UU
- **Pacchetti di installazione:** pacchetti Linux, file CAB InstallShield e Microsoft
- **File immagine:** GIF, JPEG, PNG, TIFF, AutoCAD, Photoshop, Bitmap, Visio, Digital RAW e icone di Windows
- **File audio:** WAV, MIDI, RealAudio, Dolby Digital AC-3, MP3, MP4, MOD, RealAudio, SHOUTCast e altri
- **File video:** AVI, Flash, QuickTime, Real Media, MPEG-4, Vivo, Digital Video (DV), Motion JPEG e altri
- **Altri file e applicazioni:** database, fogli di calcolo, fax, applicazioni web, tipi di carattere, file eseguibili, applicazioni Microsoft Office, giochi e strumenti di sviluppo software
- **Altri protocolli:** stampante di rete, accesso alla shell, VoIP e peer-to-peer

Esempi di utilizzo

L'appliance McAfee Application Data Monitor è in grado di rilevare varie attività non autorizzate, violazioni delle policy, furti e frodi. Ad esempio:

Furto di informazioni riservate

Un impiegato registrato come prossi@azienda.it invia un'email a complice@gmail.com. L'email contiene il file shoo.doc che include le parole "formula segreta". L'email viene inviata alle 12:20 dall'host desktop0232 (192.168.0.36) usando il server SMTP (10.0.2.13) con oggetto: capito.

Uso di applicazioni non autorizzate

Un dipendente viola la policy trasferendo musica con un'applicazione di condivisione file peer-to-peer che ha installato. Invia file di grandi dimensioni durante l'orario di lavoro, consumando larghezza di banda preziosa. Un'ulteriore indagine scopre la reiterazione della violazione da parte del dipendente. Questi usa Jabber e IRC ed esegue un server web non autorizzato sul proprio computer.

Perditempo online sul posto di lavoro

Un'altra dipendente fa trading di nascosto. Durante la giornata lavorativa si collega ai siti di trading finanziario, in media per un'ora ogni mattina e ogni pomeriggio. Utilizza inoltre il sistema VoIP (SIP) aziendale per fare in media sei chiamate al giorno, oltre a passare ore su Yahoo! Messenger come "traderpaolo" chiacchierando con "traderroberto" e "tradergiulia."

Utenti con password deboli

La policy di sicurezza della tua azienda richiede l'uso di password efficaci per tutti gli account utente di sistemi e applicazioni. Gli account di Microsoft Active Directory sono gestiti in modo rigoroso. Tuttavia, su server FTP, server di posta e applicazioni web critiche che non usano Active Directory vengono utilizzate decine di password deboli.

Ulteriori informazioni

Ulteriori informazioni sono disponibili sul sito **www.mcafee.com/siem**.

McAfee
Together is power.

Via Fantoli, 7
20138 Milano
Italy
(+39) 02 554171
www.mcafee.com/it

61322ds_app-data-monitor_0914
SETTEMBRE 2014