

# McAfee Application Control

**Riduci il rischio legato alle applicazioni non autorizzate per controllare endpoint, server e dispositivi a utilizzo fisso.**

Le minacce avanzate persistenti (APT) tramite attacco remoto o social engineering rendono sempre più difficile proteggere la tua azienda. McAfee® Application Control ti aiuta a superare in astuzia i criminali informatici e a mantenere produttiva e al sicuro l'azienda. Utilizzando un modello di affidabilità dinamico e funzioni di sicurezza innovative, come intelligence globale e locale sulla reputazione, analisi comportamentale in tempo reale e immunizzazione automatica degli endpoint, questa soluzione di McAfee sventa immediatamente le APT, senza richiedere una gestione impegnativa di elenchi o aggiornamenti delle firme. Se sei intransigente nei confronti delle minacce zero-day, dai un'occhiata a McAfee Application Control.

## Whitelisting intelligente

McAfee Application Control previene gli attacchi zero-day e le minacce APT bloccando l'esecuzione di applicazioni non autorizzate. Utilizzando la nostra funzione di inventario, è possibile individuare e gestire con facilità i file relativi alle applicazioni. Raggruppa i file binari (.EXE, .DLL, driver e script) all'interno dell'azienda in base ad applicazione e fornitore, li visualizza in un formato gerarchico intuitivo e li classifica in modo intelligente in applicazioni note, sconosciute e notoriamente pericolose. Utilizzando il whitelisting, puoi prevenire gli attacchi da parte di malware sconosciuto abilitando l'esecuzione solo di applicazioni classificate come notoriamente non pericolose.

## Implementazione del corretto stato di sicurezza

Poiché gli utenti richiedono una maggiore flessibilità nell'utilizzo di applicazioni nel loro ambiente professionale sociale e cloud, McAfee Application Control offre alle aziende tre opzioni per sfruttare al meglio la propria strategia di whitelisting per prevenire le minacce come illustrato qui di seguito.

## Vantaggi principali

- Protegge da attacchi zero-day e da minacce persistenti avanzate senza necessità di aggiornamenti delle firme.
- Sfrutta McAfee Global Threat Intelligence e McAfee Threat Intelligence Exchange per fornire la reputazione globale e locale di file e applicazioni.
- Rafforza la sicurezza e riduci i costi di possesso grazie al whitelisting dinamico che accetta automaticamente nuovo software aggiunto tramite i tuoi canali fidati.
- Controlla in modo efficiente l'accesso alle applicazioni con la piattaforma di gestione centralizzata del software McAfee® ePolicy Orchestrator® (McAfee ePO™), una piattaforma centralizzata per la gestione delle soluzioni di sicurezza McAfee.
- Riduce i cicli di applicazione delle patch grazie a whitelisting sicuro e protezione avanzata della memoria.
- Mantiene i sistemi aggiornati con le patch più recenti utilizzando strumenti di aggiornamento affidabili.
- Applica i controlli a server connessi o non collegati, computer virtuali, endpoint, dispositivi a funzione fissa come terminali POS, e sistemi legacy come Microsoft Windows XP.

## SCHEDA TECNICA



**Figura 1.** Tre modi per sfruttare al massimo la strategia relativa alle whitelist.

### Potenti suggerimenti incorporati

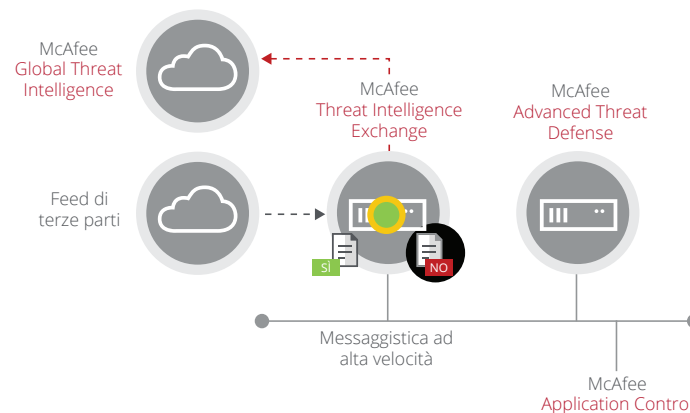
Utilizzando funzioni di ricerca dell'inventario e report predefiniti, puoi individuare e porre rimedio velocemente ai problemi legati a vulnerabilità, conformità e sicurezza all'interno del tuo ambiente. Puoi individuare approfondimenti utili, come applicazioni aggiunte, file binari non certificati, file con reputazione sconosciuta e sistemi su cui operano versioni obsolete di software, per individuare più rapidamente le vulnerabilità e convalidare la conformità delle licenze software.

### Una risposta completa e rapida

Il whitelisting viene potenziato con l'intelligence globale sulle minacce di McAfee Global Threat Intelligence (McAfee GTI), un'esclusiva tecnologia McAfee che traccia la reputazione di file, messaggi e mittenti in tempo reale tramite milioni di sensori sparsi in tutto il mondo.

McAfee Application Control utilizza questa conoscenza per stabilire la reputazione dei file presenti nell'ambiente di elaborazione, classificandoli come autorizzati, pericolosi e sconosciuti.

Quando distribuito insieme a McAfee Threat Intelligence Exchange, un modulo opzionale venduto separatamente, McAfee Application Control aggiorna la whitelist in base all'intelligence locale sulla reputazione per combattere le minacce all'istante. Utilizzando McAfee Threat Intelligence Exchange, McAfee Application Control si coordina con McAfee Advanced Threat Defense per analizzare dinamicamente il comportamento di applicazioni sconosciute in una sandbox e immunizzare gli endpoint da malware appena rilevato.



**Figura 2.** McAfee GTI monitora costantemente la reputazione di file e mittenti. Quando distribuito con McAfee Threat Intelligence Exchange, McAfee Application Control aggiorna automaticamente la whitelist sulla base dell'intelligence locale sulla reputazione e può coordinarsi con McAfee Advanced Threat Defense se sono necessarie maggiori informazioni relativamente a un file.

### Vantaggi principali (continua)

- Autorizza le nuove applicazioni in base al punteggio dell'applicazione o tramite approvazione automatica per una migliore continuità aziendale.
- Non intralcia la produttività degli utenti né le prestazioni del server grazie a una soluzione che richiede un basso utilizzo di risorse.
- Protegge con facilità i sistemi legacy e gli investimenti in tecnologie moderne.

### Piattaforme supportate

#### Microsoft Windows (a 32 bit e 64 bit)

- Integrato: Windows XPE, 7 Embedded, WEPOS, POSReady 2009, WES 2009, Embedded 8, 8.1 Industry, 10
- Server: Windows Server 2008, 2008 R2, 2012, 2012 R2
- Desktop: Windows NT, 2000, XP, Vista, 7, 8, 8.1, 10

#### Linux

- Red Hat/CentOS 5, 6, 7
- SUSE/openSUSE 10, 11
- Oracle Enterprise Linux 5, 6, 7
- Ubuntu 12.04

## SCHEDA TECNICA

### Nessun impatto sulla continuità aziendale

Per evitare interferenze con la continuità aziendale, le nuove applicazioni vengono autorizzate in automatico sulla base della reputazione dell'applicazione. Per le applicazioni sconosciute, un'interfaccia consiglia le nuove policy aggiornate sulla base dei percorsi di esecuzione a livello di endpoint. Si tratta di un modo eccellente per gestire le eccezioni generate dalle applicazioni bloccate. Dopo aver analizzato le eccezioni e i dettagli dell'applicazione bloccata, semplicemente provvede ad approvare ed inserire in whitelist il file o lo ignora per bloccare l'applicazione.

### Aiuta gli utenti a diventare parte della soluzione

Per le applicazioni sconosciute, McAfee Application Control offre ai reparti IT diversi modi per consentire agli utenti l'installazione di nuove applicazioni:

- **Avvisi agli utenti**—Gli utenti possono ricevere messaggi popup informativi che spiegano perché non è concesso l'accesso ad applicazioni non autorizzate. Questi messaggi indicano agli utenti di richiedere approvazioni via email o tramite helpdesk.
- **Utenti con diritti di approvazione automatici**—Gli utenti con questo privilegio possono installare nuovo software senza aspettare l'approvazione da parte dell'IT. Il personale IT può comunque verificare tali approvazioni automatiche e creare policy aziendali per bloccare o autorizzare l'app su tutti i sistemi.

### Mantieni aggiornati i sistemi

Sappiamo che mantenere i sistemi aggiornati con le patch più recenti è importante. Per questo motivo offriamo un modello di affidabilità dinamico per aggiornare in automatico i tuoi sistemi senza alcun impatto sulla continuità aziendale. Mantieni i tuoi sistemi aggiornati utilizzando utenti fidati, certificati, processi e directory. McAfee Application Control evita inoltre che le applicazioni inserite in whitelist vengano sfruttate tramite attacchi di buffer overflow della memoria su sistemi Microsoft Windows a 32 e 64 bit.

### Controllo avanzato dell'esecuzione

Per una maggiore protezione, McAfee Application Control permette di combinare regole sulla base di criteri quali: nome file, nome processo, nome processo padre, parametri linea di comando e nome utente. È possibile utilizzare il controllo avanzato dell'esecuzione per bloccare gli attacchi che aggirano l'I/O (Input/Output) dei file, bloccare la modalità interattiva per gli interpreti di sistema e prevenire lo sfruttamento dagli strumenti di sistema. Inoltre, si ha disposizione l'algoritmo SHA-256 più potente e solido per la creazione delle policy.

## SCHEDA TECNICA

### Software McAfee ePolicy Orchestrator: un unico punto di vista

Il software McAfee ePO consolida e centralizza la gestione, fornendo una visione globale della sicurezza dell'azienda senza punti ciechi. Questa premiata piattaforma integra il software McAfee Application Control con McAfee Host Intrusion Prevention e altri prodotti di sicurezza McAfee, tra cui l'antimalware per il blacklisting. L'installazione e l'aggiornamento in un solo passaggio della distribuzione di McAfee Application Control possono essere effettuati anche da Microsoft System Center.

### La modalità di sorveglianza: come il software osserva e apprende

La modalità di sorveglianza aiuta a individuare le policy per gli ambienti desktop dinamici senza la necessità di applicare un blocco tramite whitelisting. Permette di distribuire gradualmente McAfee Application Control in ambienti di pre-produzione o produzione preliminare senza violare le applicazioni. Tramite McAfee Application Control, gli amministratori possono utilizzare un'unica pagina di rilevamento di policy che consente loro di definire le policy per richieste di approvazione automatica e sorveglianza.

### Protezione dei sistemi legacy e investimenti in tecnologie recenti

Devi proteggere i sistemi operativi più obsoleti, come Microsoft Windows NT, 2000 e XP? Sebbene Microsoft e altri fornitori di soluzioni di sicurezza non supportino più questi sistemi legacy, con McAfee Application Control sei coperto. Inoltre, McAfee Application Control supporta i sistemi operativi più recenti come Microsoft Windows 10.

### Agisci

Per maggiori informazioni, visita [www.mcafee.com/it/products/application-control.aspx](http://www.mcafee.com/it/products/application-control.aspx) o chiamaci al numero +39 02554171.



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

McAfee, il logo McAfee, ePolicy Orchestrator e McAfee ePO sono marchi registrati o marchi di McAfee, LLC o sue filiali negli Stati Uniti e in altri Paesi. Altri marchi e denominazioni potrebbero essere rivendicati come proprietà di terzi. Copyright © 2017 McAfee, LLC. 2183\_1216  
DICEMBRE 2016