McAfee Network Security Platform

Un approccio alla sicurezza di rete unico e intelligente

McAfee® Network Security Platform è una soluzione di sicurezza intelligente e unica, in grado di scoprire e bloccare le minacce più sofisticate presenti nella rete. Utilizzando tecniche avanzate di rilevamento ed emulazione, va ben oltre la mera corrispondenza degli schemi per difendere dagli attacchi occulti con estrema accuratezza. Questa piattaforma hardware di nuova generazione può raggiungere una velocità superiore ai 40 Gbit/s con un singolo dispositivo, per soddisfare le esigenze delle reti più esigenti. Il nostro approccio alla gestione della sicurezza ottimizza le operazioni unendo i feed in tempo reale di McAfee Global Threat Intelligence (McAfee GTI) ai dati contestuali completi riferiti a utenti, dispositivi e applicazioni per una risposta rapida e accurata agli attacchi che si sviluppano sulle reti.

Vantaggi principali

Prevenzione avanzata e senza confronti contro le minacce

- Analisi malware avanzata, senza firme
- Browser in linea ed emulazione di JavaScript
- Rilevamento avanzato dei callback di botnet e malware
- Analisi basata sul comportamento e protezione DDoS
- Integrazione con McAfee Advanced Threat Defense

Architettura di protezione unificata

- Condivisione in tempo reale delle informazioni sulle minacce tramite McAfee Threat Intelligence Exchange (TIE)
- Contesto degli endpoint tramite ePolicy Orchestrator® (McAfee ePO™)
- Correlazione processi degli endpoint tramite McAfee Endpoint Intelligence Agent
- Condivisione dati e messa in quarantena tramite McAfee Enterprise Security Manager (SIEM)

Proteggiti contro la minaccia dei moderni virus occulti

La rete della tua azienda deve affrontare gli attacchi dei virus occulti avanzati in grado di oltrepassare i tradizionali metodi di rilevamento e di causare violazioni e interruzioni della rete. Purtroppo molte aziende non dispongono delle risorse finanziarie e operative per implementare e gestire la combinazione di strumenti e tecnologie necessarie per creare una difesa adeguata a questi attacchi.

McAfee Network Security Platform è una piattaforma di sicurezza di rete integrata che unisce la prevenzione intelligente delle minacce a una gestione della sicurezza intuitiva, così da migliorare l'accuratezza del rilevamento e ottimizzare le operazioni di sicurezza. Offre una copertura senza paragoni nel settore, contro le minacce avanzate, i callback del malware, le minacce zero-day e gli attacchi denial of service.

Appositamente studiata per l'integrazione con l'architettura McAfee di protezione unificata, McAfee Network Security Platform utilizza i dati di sicurezza provenienti da tutta l'azienda per aiutarti a chiudere le falle nella protezione, che spesso non vengono rilevate dalle altre soluzioni di sicurezza composite.

Prevenzione senza confronti contro le minacce

McAfee Network Security Platform si basa su un'architettura di ispezione di nuova generazione progettata per effettuare un'ispezione profonda del traffico di rete pur mantenendo la normale velocità della linea. Utilizza una combinazione di tecniche di ispezione avanzate (tra cui l'analisi completa del protocollo, la reputazione delle minacce, l'analisi del comportamento e l'analisi avanzata del malware) per rilevare e impedire gli attacchi conosciuti e quelli di tipo zero-day sulla rete.

intel Security

Vantaggi principali (segue)

- Analisi dei rischi dell'host tramite McAfee Vulnerability Manager
- Rilevamento preventivo del malware tramite McAfee GTI

Prestazioni e disponibilità

- Architettura di nuova generazione
- Fino a 40 Gbit/s di velocità
- Ispezione SSL con prestazioni senza confronti
- Affidabilità leader del settore
- Disponibilità attivo-attivo e attivo-passivo

Gestione intelligente della sicurezza

- Correlazione e priorità intelligenti degli allarmi
- Robuste dashboard di indagine sul malware
- Flussi di lavoro preconfigurati per le indagini
- Gestione scalabile e basata sul web

Visibilità e controllo

- Identificazione delle applicazioni
- Identificazione degli utenti
- Identificazione dei dispositivi

Difesa completa contro il malware

Nessuna tecnologia di rilevamento del malware può bloccare da sola tutti gli attacchi: per questo motivo McAfee Network Security Platform include diversi motori di rilevamento con e senza firme per impedire al malware di danneggiare la tua rete. La soluzione combina la reputazione dei file di McAfee GTI e l'analisi approfondita dei file con l'ispezione JavaScript e un motore anti-malware avanzato per rilevare il malware personalizzato e altri attacchi di virus occulti.

Architettura di protezione unificata

Avere il controllo dei dati di cui hai bisogno non è mai stato più semplice. McAfee offre un'integrazione in tempo reale con McAfee ePO e McAfee Enterprise Security Manager per una correlazione in tempo reale degli eventi di rete su tutte le fonti pertinenti. Grazie all'integrazione con il software McAfee ePO e con McAfee Enterprise Security Manager, McAfee Network Security Platform restituisce un quadro accurato delle minacce, del modo in cui si relazionano con i dispositivi e gli utenti e quali rappresentano il maggiore rischio per l'azienda. La soluzione integra i dettagli dei dispositivi, le informazioni degli utenti, lo stato complessivo della sicurezza degli endpoint, le valutazioni di vulnerabilità e altre informazioni dettagliate che consentono alle aziende di comprendere la gravità delle minacce e i fattori di rischio per l'attività aziendale.

Prestazioni e scalabilità

Il meglio possibile: sicurezza e prestazioni elevate. McAfee Network Security Platform combina in un unico dispositivo un'architettura di analisi single-pass, basata su protocollo, con hardware di classe carrier realizzato appositamente per un'analisi del mondo reale ad oltre 40 Gbit/s. La sua architettura ultra efficiente preserva le prestazioni indipendentemente dalle impostazioni di sicurezza, mentre altri sistemi di prevenzione delle intrusioni (IPS) possono subire una riduzione del throughput fino al 50% con policy che danno priorità alla sicurezza rispetto alle prestazioni.

Visibilità e controllo

Prendi decisioni informate riguardo alle applicazioni e ai protocolli presenti sulla rete dell'azienda. McAfee Network Security Platform è la prima e unica soluzione IPS a riunire funzioni avanzate di prevenzione delle minacce e consapevolezza delle applicazioni in un unico motore decisionale sulla sicurezza. Mettiamo in relazione l'attività delle minacce con l'utilizzo delle applicazioni, inclusa la visibilità al livello 7 di oltre 1.500 applicazioni e protocolli, per permetterti di prendere decisioni informate su quali applicazioni autorizzare sulla rete. Oltre all'identificazione delle applicazioni, McAfee Network Security Platform offre visibilità su utenti e dispositivi. Assegna delle priorità a host e utenti a rischio e considera anche le botnet attive, tramite l'identificazione di comportamenti di rete anomali.

Gestione intelligente della sicurezza

Ottieni il massimo dal tuo investimento in sicurezza tramite una gestione intelligente della sicurezza di rete. McAfee Network Security Manager consente una gestione scalabile e basata sul web di un numero di appliance di sicurezza di rete compreso tra due e diverse centinaia. Offre dei flussi di lavoro a divulgazione progressiva in grado di indicare agli amministratori gli avvisi pertinenti e delle dashboard di sicurezza di facile utilizzo che automatizzano gli eventi sulla base della gravità e della pertinenza degli avvisi. McAfee Network Security Platform si integra con il software McAfee ePO per fornire all'organizzazione una vista consolidata del rischio e della conformità dell'intera azienda e include valutazioni aggiornate minuto per minuto dell'infrastruttura a rischio sulla base delle vulnerabilità del sistema, delle difese di rete e dei livelli di sicurezza degli endpoint.

McAfee Network Security Platform permette di:

Chiudere le falle nella sicurezza

- Bloccare l'attività di rete dannosa
- Evitare gli attacchi occulti
- Rilevare il malware avanzato

Ridurre i problemi di gestione

- Assegnare automaticamente le priorità agli eventi
- Ottimizzare i flussi di lavoro di indagine
- Eliminare le operazioni di messa a punto non necessarie

Adattarsi alla rete

- Connettività di 1, 10 e 40 Gigabit Ethernet
- Scalabile fino a 40 Gbit/s
- Disponibilità attivo-attivo e attivo-passivo

Funzionalità aggiuntive

Prevenzione delle minacce avanzate

- Motore di emulazione McAfee Gateway Anti Malware (GAM)
- Motore di emulazione PDF Javascript
- Motore di analisi comportamentale Adobe Flash
- Protezione avanzata dalle tecniche di evasione
- Analisi della reputazione delle minacce mobili e del cloud

Protezione dai callback di botnet e malware

- Rilevamento dei callback fast flux DNS/DGA
- Sinkholing DNS
- Rilevamento euristico dei bot
- Correlazione degli attacchi multipli
- Database di controllo e comando

Prevenzione avanzata delle intrusioni

- Deframmentazione IP e riassemblaggio del flusso TCP
- Firme McAfee, open-source e definite dall'utente
- Messa in quarantena dell'host e limitazione della velocità
- Ispezione degli ambienti virtuali

Prevenzione attacchi DoS e DDoS

- Rilevamento basato su soglie ed euristica
- Limitazione della connessione basata su host
- Rilevamento ad autoapprendimento, basato su profili

McAfee GTI

- Reputazione dei file
- Reputazione degli IP
- Reputazione di applicazione e protocollo
- Localizzazione geografica

Elevata disponibilità

- Attivo-attivo e attivo-passivo con failover stateful
- Fail-open esterno (attivo)
- Fail-open interno

Supporto per il tunneling dei protocolli

- IPv6
- Tunnel V4-in-V4, V4-in-V6, V6-in-V4 e V6-in-V6
- MPLS
- GRE
- Q-in-Q Double VLAN

McAfee Network Security Manager

- Gestione multilivello (fino a 1.000 sensori)
- Autenticazione utente (Radius e LDAP)
- Failover e fail-back automatici
- Disaster recovery dei dati critici di configurazione
- Gestione gerarchica e centralizzata delle policy

Specifiche della soluzione McAfee Network Security Platform

	Hardware di nuova generazione		
			
Componenti hardware del sensore	**NS9300**	**NS9200**	**NS9100**
Prestazioni			
Prestazioni aggregate	40 Gbit/s	20 Gbit/s	10 Gbit/s
Throughput massimo (Pacchetti UDP 1.512 Byte)	Fino a 70 Gbit/s	Fino a 35 Gbit/s	Fino a 30 Gbit/s
Numero massimo di connessioni contemporanee	32.000.000	16.000.000	13.000.000
Connessioni al secondo	1.000.000	575.000	450.000
Connessioni HTTP al secondo	750.000	375.000	260.000
Throughput con decodifica SSL (basata su traffico SSL al 10%)	40 Gbit/s	20 Gbit/s	10 Gbit/s
Livello massimo del flusso SSL	3.200.000	1.600.000	1.200.000
Chiavi SSL importate	1.024	1.024	1.024
Latenza tipica	Meno di 100 µs	Meno di 100 µs	Meno di 100 µs
Numero di sistemi IPS virtuali	1.000	1.000	1.000
Numero massimo profili DoS	5.000	5.000	5.000
Regole ACL	20.000	20.000	20.000
Porte			
Gigabit Ethernet fissa - Porte in rame (fail-open interno)	16	8	8
Porte fisse 10 GbE/1 GbE (SFP+)	—	—	—
40 Gigabit Ethernet fissa	—	2	2
Slot I/O di rete	4	2	2
Moduli I/O di rete (sei opzioni)	4 porte 10 GigE/1 GigE SR ottico, 50 micron con fail open, 4 porte 10 GigE/1 GigE SR ottico, 62,5 micron con fail open, 4 porte (QSFP+) 40 GbE, 2 porte (QSFP+) 40 GbE, 8 porte (SFP+/SFP) 10 GbE/1 GbE o 6 porte (RJ45) 1 GbE (con fail-open interno)		
10 Gigabit Ethernet	Fino a 32	Fino a 16	Fino a 16
40 Gigabit Ethernet	Fino a 16	Fino a 10	Fino a 10
Porte di risposta dedicate (RJ45)	1 (10G/1G/100M)	1 (10G/1G/100M)	1 (10G/1G/100M)
Porte di gestione dedicate (RJ45)	1 (10G/1G/100M)	1 (10G/1G/100M)	1 (10G/1G/100M)
Porte di archiviazione dedicate (RJ45)	1 (10G/1G/100M)	1 (10G/1G/100M)	1 (10G/1G/100M)
Fisiche			
Dimensioni	2 x montabile in rack 2RU 43,79 cm (L) x 17,48 cm (A) x 73,05 cm (P)	Montabile in rack 2RU 43,79 cm (L) x 8,74 cm (A) x 73,05 cm (P)	Montabile in rack 2RU 43,79 cm (L) x 8,74 cm (A) x 73,05 cm (P)
Peso	60,8 kg	30,4 kg	30,4 kg
Archiviazione	600 GB (2 x Dual Solid State 300 GB in configurazione RAID 1)	Dual Solid State 300 GB in configurazione RAID 1	Dual Solid State 300 GB in configurazione RAID 1
Massimo consumo di elettricità	2.260 W	1.130 W	1.130 W
Alimentazione c.c. disponibile	Opzionale	Opzionale	Opzionale
Alimentatore ridondante	Compreso	Compreso	Opzionale
Alimentazione	100-240 VCA (50/60 Hz)		
Temperatura	Da 0 °C a 35 °C (operativa). Da –40 °C a 70 °C (non operativa)		
Umidità relativa (senza condensa)	Operativa: 10% a 90% (operativa). Da 5% a 95% (non operativa)		
Altitudine	Da 0 a 3.000 m		
Certificazioni di sicurezza	Licenze e report UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB che coprono tutte le differenze nazionali.		
Certificazione EMI	FCC Part 15, Classe A (CFR 47) (USA), ICES-003 Classe A (Canada), EN55022 Classe A (Europa), CISPR22 Classe A (Internazionale)		

Specifiche di Network Security Platform continua

Componenti hardware del sensore	 NS7300	 NS7200	 NS7100
Prestazioni			
Prestazioni aggregate	5 Gbit/s	3 Gbit/s	1,5 Gbit/s
Velocità massima (Pacchetti UDP 1.512 Byte)	Fino a 15 Gbit/s	Fino a 10 Gbit/s	Fino a 5 Gbit/s
Numero massimo di connessioni contemporanee	10.000.000	5.000.000	3.000.000
Connessioni al secondo	225.000	200.000	135.000
Connessioni HTTP al secondo	135.000	128.000	115.000
Throughput con decodifica SSL (basata su traffico SSL al 10%)	5 Gbit/s	3 Gbit/s	1,5 Gbit/s
Livello massimo del flusso SSL	500.000	400.000	250.000
Chiavi SSL importate	1.024	1.024	1.024
Latenza tipica	Meno di 100 µs	Meno di 100 µs	Meno di 100 µs
Numero di sistemi IPS virtuali	1.000	1.000	1.000
Numero massimo profili DoS	5.000	5.000	5.000
Regole ACL	5.000	3.000	3.000
Porte			
Gigabit Ethernet fissa - Porte in rame (fail-open interno)	8	8	8
Porte fisse 10 GbE/1 GbE (SFP+) (supporto fail-open passivo esterno)	2	2	2
40 Gigabit Ethernet fissa	—	—	—
Slot I/O di rete	2	2	2
Moduli I/O di rete (cinque opzioni)	4 porte 10 GbE/1 GbE SR ottico 50 micron con fail open, 4 porte 10 GbE/1 GbE SR ottico 62,5 micron con fail open, 4 porte 10 GbE/1 GbE LR ottico con fail open, 8 porte (SFP+/SFP) 10 GbE/1 GbE, oppure 6 porte (RJ45) 1 GbE con fail open interno		
10 Gigabit Ethernet	Fino a 18	Fino a 18	Fino a 18
40 Gigabit Ethernet	—	—	—
Porte di risposta dedicate (RJ45)	1 (1G/100M/10M)	1 (1G/100M/10M)	1 (1G/100M/10M)
Porte di gestione dedicate (RJ45)	1 (1G/100M/10M)	1 (1G/100M/10M)	1 (1G/100M/10M)
Porte di archiviazione dedicate (RJ45)	1 (1G/100M/10M)	1 (1G/100M/10M)	1 (1G/100M/10M)
Caratteristiche fisiche			
Dimensioni	Montabile in rack 1RU da 44,45 (L) x 4,29 (A) x 73,41 (P) cm	Montabile in rack 1RU da 44,45 (L) x 4,29 (A) x 73,41 (P) cm	Montabile in rack 1RU da 44,45 (L) x 4,29 (A) x 73,41 (P) cm
Peso	14 kg	14 kg	13 kg
Archiviazione	Stato solido 160 GB	Stato solido 160 GB	Stato solido 160 GB
Massimo consumo di elettricità	350 W	350 W	250 W
Alimentazione c.c. disponibile	Opzionale	Opzionale	Opzionale
Alimentatore ridondante	Opzionale	Opzionale	Opzionale
Alimentazione	100-240 VCA (50/60 Hz)		
Temperatura	Da 0 °C a 35 °C (operativa). Da –40 °C a 70 °C (non operativa)		
Umidità relativa (senza condensa)	Operativa: da 10% a 90%. Non operativa: da 5% a 95%		
Altitudine	Da 0 a 3.000 m		
Certificazioni di sicurezza	Licenze e report UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB che coprono tutte le differenze nazionali.		
Certificazione EMI	FCC Part 15, Classe A (CFR 47) (USA), ICES-003 Classe A (Canada), EN55022 Classe A (Europa), CISPR22 Classe A (Internazionale)		

Specifiche di Network Security Platform continua

Componenti hardware del sensore	NS5200	NS5100
Prestazioni		
Prestazioni aggregate	1 Gbit/s	600 Mbit/s
Velocità massima (Pacchetti UDP 1.512 Byte)	Fino a 3 Gbit/s	Fino a 1,5 Gbit/s
Numero massimo di connessioni contemporanee	1.350.000	750.000
Connessioni al secondo	45.000	40.000
Connessioni HTTP al secondo	30.000	25.000
Throughput con decodifica SSL (basata su traffico SSL al 10%)	1 Gbit/s	600 Mbit/s
Livello massimo del flusso SSL	75.000	40.000
Chiavi SSL importate	1.024	1.024
Latenza tipica	Meno di 100 µs	Meno di 100 µs
Numero di sistemi IPS virtuali	1.000	100
Numero massimo profili DoS	5.000	300
Regole ACL	2.000	2.000
Porte		
Gigabit Ethernet fissa - Porte in rame (fail-open interno)	8	8
Porte fisse 1 GbE (SFP+)	12	12
Porte fisse 10 GbE/1 GbE (SFP+) (supporto fail-open passivo esterno)	2	2
40 Gigabit Ethernet fissa	—	—
Slot I/O di rete	—	—
Moduli I/O di rete	—	—
10 Gigabit Ethernet	—	—
40 Gigabit Ethernet	—	—
Porte di risposta dedicate (RJ45)	1 (1G/100M)	1 (1G/100M)
Porte di gestione dedicate (RJ45)	1 (1G/100M)	1 (1G/100M)
Porte di archiviazione dedicate (RJ45)	1 (1G/100M)	1 (1G/100M)
Fisica		
Dimensioni	Montabile su rack 1RU da 43,82 (L) x 4,45 (A) x 62,55 (P) cm	Montabile su rack 1RU da 43,82 (L) x 4,45 (A) x 62,55 (P) cm
Peso	9,98 kg	9,98 kg
Archiviazione	Stato solido 80 GB	Stato solido 80 GB
Massimo consumo di elettricità	225 W	225 W
Alimentazione c.c. disponibile	Opzionale	Opzionale
Alimentatore ridondante	Opzionale	Opzionale
Alimentazione	100-240 VCA (50/60 Hz)	
Temperatura	Da 0 °C a 35 °C (operativa). Da –40 °C a 70 °C (non operativa)	
Umidità relativa (senza condensa)	Operativa: da 10% a 90%. Non operativa: da 5% a 95%	
Altitudine	Da 0 a 3.000 m	
Certificazioni di sicurezza	Licenze e report UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB che coprono tutte le differenze nazionali.	
Certificazione EMI	FCC Part 15, Classe A (CFR 47) (USA), ICES-003 Classe A (Canada), EN55022 Classe A (Europa), CISPR22 Classe A (Internazionale)	

Specifiche di Network Security Platform continua

Componenti hardware del sensore	 NS3200	 NS3100
Prestazioni		
Prestazioni aggregate	200 Mbit/s	100 Mbit/s
Velocità massima (Pacchetti UDP 1.512 Byte)	Fino a 1 Gbps	Fino a 600 Mbps
Numero massimo di connessioni contemporanee	80.000	40.000
Connessioni al secondo	20.000	15.000
Connessioni HTTP al secondo	15.000	12.000
Throughput con decodifica SSL (basata su traffico SSL al 10%)	—	—
Livello massimo del flusso SSL	—	—
Chiavi SSL importate	—	—
Latenza tipica	Meno di 100 µs	Meno di 100 µs
Numero di sistemi IPS virtuali	32	16
Numero massimo profili DoS	128	128
Regole ACL	1.000	1.000
Porte		
Gigabit Ethernet fissa - Porte in rame (fail-open interno)	8	8
Porte fisse 1 GbE (SFP+)	—	—
Porte fisse 10 GbE/1 GbE (SFP+) (supporto fail-open passivo esterno)	—	—
40 Gigabit Ethernet fissa	—	—
Slot I/O di rete	—	—
Moduli I/O di rete	—	—
10 Gigabit Ethernet	—	—
40 Gigabit Ethernet	—	—
Porte di risposta dedicate (RJ45)	1 (1G/100M)	1 (1G/100M)
Porte di gestione dedicate (RJ45)	1 (1G/100M)	1 (1G/100M)
Porte di archiviazione dedicate (RJ45)	1 (1G/100M)	1 (1G/100M)
Fisica		
Dimensioni	Montabile su rack 1RU da 44,15 (L) x 4,45 (A) x 27,94 (P) cm	Montabile su rack 1RU da 44,15 (L) x 4,45 (A) x 27,94 (P) cm
Peso	3,67 kg	3,67 kg
Archiviazione	Stato solido 30 GB	Stato solido 30 GB
Massimo consumo di elettricità	100 W	100 W
Alimentazione c.c. disponibile	—	—
Alimentatore ridondante	—	—
Alimentazione	100-240 VCA (50/60 Hz)	
Temperatura	Da 0 °C a 35 °C (operativa). Da –40 °C a 70 °C (non operativa)	
Umidità relativa (senza condensa)	Operativa: da 10% a 90%. Non operativa: da 5% a 95%	
Altitudine	Da 0 a 3.000 m	
Certificazioni di sicurezza	Licenze e report UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB che coprono tutte le differenze nazionali.	
Certificazione EMI	FCC Part 15, Classe A (CFR 47) (USA), ICES-003 Classe A (Canada), EN55022 Classe A (Europa), CISPR22 Classe A (Internazionale)	

McAfee. Part of Intel Security.
Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com