



## Descrizione tecnica

**NVIDIA Firewall**  
Sicurezza dei PC  
e difesa dagli hacker

# Sicurezza dei PC e difesa dagli hacker

---

## Introduzione

I computer costituiscono parte integrante della vita quotidiana di numerosissime persone, sia per esigenze lavorative che per il tempo libero e l'intrattenimento. Questi dispositivi contengono ogni tipo di informazioni utili, fatto che li rende un bersaglio ideale per gli hacker. Questo fatto è il motivo principale per il quale la sicurezza dei computer è diventata uno dei problemi principali che ci troviamo ad affrontare oggi.

La sicurezza dei computer si articola su tre componenti indipendenti fra loro: un firewall, l'individuazione delle intrusioni e una protezione anti-virus.

Il firewall è il componente portante di tutte le soluzioni di sicurezza per i computer. Questo dispositivo garantisce che solo i pacchetti dati conformi alle politiche definite possano oltrepassarlo. Per conseguire questo risultato, il firewall esamina ogni pacchetto dati che tenta di attraversarlo e determina se il suddetto pacchetto abbia attributi ammissibili. In caso negativo, il pacchetto viene bloccato. L'integrazione nel software del driver del PC della funzionalità firewall limita drasticamente la possibilità di accesso non autorizzato, sia via Intranet che via Internet.

NVIDIA® Firewall è il primo firewall che si basa sul motore di networking sicuro NVIDIA ActiveArmor™. Di conseguenza, NVIDIA Firewall ha prestazioni di sistema eccellenti pur con un utilizzo della CPU davvero minimo. Allo stesso tempo, questa soluzione aumenta la sicurezza complessiva offrendo funzioni di ispezione approfondita dei pacchetti a base hardware, protezione instant-on e funzionalità anti-manomissione.

---

## Firewall

### Finalità operative

I dati in rete si compongono di *pacchetti* le cui intestazioni contengono meta-informazioni. Queste meta-informazioni consentono al pacchetto di essere consegnato su una subnetwork (intestazione livello Data Link), una internetwork

(intestazione livello Network) e nel processo corretto di un host (intestazione livello Transport). Quando una macchina è collegata a Internet, qualsiasi altra macchina su Internet può inviarle un pacchetto se questa macchina remota conosce l'indirizzo IP della macchina di destinazione.

La maggior parte dei pacchetti sono innocui, ma occasionalmente qualcuno tenta di inviare pacchetti che sfruttano bug nel software di protocollo o del sistema operativo dell'host di destinazione. La finalità di questi pacchetti è quella di disabilitare l'host (un tipo di attacco noto come "denial of service"), o di permettere l'accesso non autorizzato all'host.

La maggior parte delle reti aziendali e alcune di quelle domestiche hanno una connessione a Internet ben definita. La connessione consiste di un numero limitato di punti di connessione (modem DSL) tramite i quali i pacchetti degli host interni possono raggiungere Internet e viceversa. Per controllare quali pacchetti possono attraversare questo confine virtuale, è stato creato il concetto di *firewall*.

## Modalità operative

I firewall permettono di filtrare il traffico di rete, sulla base di una varietà di criteri. Il modo più ovvio per filtrare il traffico consiste nel tipo di pacchetto. Utilizzando i numeri di porta TCP o UDP di un pacchetto, il firewall permette o nega l'accesso a ogni pacchetto, decidendo sulla base di regole memorizzate nella tabella di controllo degli accessi.

Ci sono due possibili scenari per l'attività di filtratura dei pacchetti esercitata da un firewall:

- ❑ Da una parte, un firewall può lasciare passare tutti i pacchetti ad eccezione di quelli appartenenti a una lista definita (identificati da numeri di porta) che sono considerati nocivi e vengono scartati.
- ❑ Dall'altra, un firewall potrebbe essere programmato per bloccare tutti i pacchetti per default, lasciando passare solo quelli di cui è accertata l'innocuità.

La sicurezza consiste proprio nella gestione dei possibili rischi. Con la definizione della configurazione di un firewall, gli utenti limitano i rischi connessi ai pacchetti che fanno accedere alla propria rete. In generale, i firewall possono essere configurati, quindi è difficile per un aggressore determinare a priori quale tipo di traffico possa accedere a uno specifico firewall. Questo tipo di protezione garantisce quindi un certo grado di anonimità.

## Tipi di firewall

### Firewall stateless

Il firewall stateless è il tipo più elementare di firewall ed esiste, sia pure in forme diverse, sin dai primissimi anni '90. Questo tipo di firewall contiene un elenco di regole di ammissione/diniego definite in modo da permettere di oltrepassare il firewall ai soli pacchetti che corrispondono a specifiche condizioni. Le regole possono filtrare il traffico in ingresso e/o quello in uscita sulla base di tipo Ethernet,

sorgente IP o indirizzo di destinazione, opzioni IP, protocollo IP, tipo ICMP e/o valori codice, sorgente TCP o UDP, porta di destinazione e opzioni TCP.

Se il pacchetto passa questo test può attraversare la protezione, in caso contrario viene scartato. Tuttavia, tutti i pacchetti vengono sottoposti allo stesso tipo di test. Il problema di scalatura insito in questo tipo di soluzione consiste proprio nel fatto che ogni pacchetto deve essere verificato sulla base di tutte le regole. La costante aggiunta di regole ulteriori rende progressivamente più difficile l'elaborazione di ciascun pacchetto. Questo sforzo aggiuntivo finisce per ridurre le prestazioni, misurate in pacchetti al secondo, o sulla base dell'utilizzo di CPU per elaborare una data quantità di traffico. I firewall stateless risultano i più adatti a certi pacchetti, quali gli ICMP, che sono stateless per natura.

NVIDIA Firewall supporta l'ispezione stateless. La nostra soluzione è in grado di filtrare il traffico sulla base del tipo Ethernet, del protocollo IP e delle regole opzionali IP e TCP. IPv4 e IPv6 vengono trattati allo stesso modo, ogniqualvolta sia possibile. Per esempio, le opzioni IPv4 e le intestazioni dell'estensione IPv6 possono essere utilizzate entrambe come elementi del filtro.

## Firewall stateful

Un firewall stateful costituisce una variante di quelli stateless. Si tratta di un firewall che si comporta più o meno come quelli stateless quando viene stabilita una nuova connessione, dato che il protocollo (oltre a sorgente e destinazione del pacchetto) viene messo a confronto con le politiche locali.

L'ottimizzazione del firewall stateful consiste nel fatto che i pacchetti di un flusso dato vengono esaminati nel dettaglio soltanto all'inizio della connessione. Quando una nuova connessione viene considerata verificata e ammissibile, viene aggiunta una voce a una tabella di verifica dello stato di connessione. I futuri pacchetti che corrispondono a questa voce della tabella di connessione possono essere verificati in base alla tabella delle connessioni ammissibili, senza sottoporre ogni singolo pacchetto all'intera serie di regole di verifica. Il vantaggio di un firewall stateful consiste proprio nell'offerta di tutta la sicurezza di un firewall di filtratura dei pacchetti, utilizzando una frazione dei cicli di CPU della soluzione stateless.

NVIDIA Firewall supporta l'ispezione stateful del traffico TCP e UDP. Uno "stato" UDP viene determinato mediante l'osservazione dei nuovi pacchetti UDP e la creazione di stati soltanto se questi superano con successo le regole del firewall definite dall'utente.

La tecnica di investigazione prevede il calcolo di un valore di hash basato su diversi campi chiave nell'intestazione del pacchetto. I campi chiave possono includere gli indirizzi IP di sorgente e destinazione, il protocollo IP (che indica se si sta utilizzando il protocollo di layer di trasporto TCP, UDP o altri) e le porte del layer di trasporto di sorgente e destinazione. Il calcolo di una funzione hash su questi cinque valori impiega una quantità di tempo fissa (e ridotta) per ogni pacchetto.

La complessità delle regole del firewall non influenza la velocità di convalida dei pacchetti da parte del firewall. Al contrario, il firewall stateless deve invece applicare tutte le proprie regole (o un numero di regole sufficiente a raggiungere una decisione definitiva) per ciascun pacchetto. Inoltre, il suo tempo di analisi del pacchetto aumenta in modo lineare proporzionalmente al numero di regole implementate, dando luogo a una riduzione costante del numero di pacchetti inoltrati per unità di tempo.

## Gateway a livello applicativo

Un gateway sul layer dell'applicazione, o un bridge livello di trasporto, è un computer con finalità speciali che esegue servizi proxy per ciascuna applicazione cui è consentito il passaggio. Questi server proxy devono essere eccezionalmente stabili e inviolabili: ogni punto debole costituisce infatti un elemento di instabilità per l'intero sistema. Nessun pacchetto passa direttamente attraverso un gateway a livello applicativo. Dopo che un pacchetto è stato ricevuto da questo firewall, gli vengono sottratte tutte le intestazioni, ne viene esaminato il contenuto e viene poi creata una nuova serie di pacchetti su una nuova connessione con l'host di destinazione.

Un gateway a livello applicativo ha qualità di trasparenza del tutto analoghe a quelle del firewall di filtratura dei pacchetti, con la sola possibile eccezione di un ulteriore ritardo nel processo di esame. Il vantaggio di questo approccio consiste nel fatto che

esiste una “bolla d’aria” logica tra le due reti, ma questa è limitata ai soli protocolli interpretabili dal gateway.

La più importante limitazione del gateway a livello applicativo consiste nel fatto che per consentire il passaggio a un certo tipo di traffico, deve esistere un server proxy per quel protocollo. I proxy per protocolli molto diffusi quali SMTP, FTP, HTTP e TELNET sono facilmente reperibili, ma i proxy per protocolli più insoliti potrebbero non essere disponibili. Per applicazioni limitate, comunque, questi gateway costituiscono la scelta migliore per garantire l’accesso alla rete dei soli dati validi.

I firewall gateway a livello applicativo sono solitamente disposti sul margine della rete e richiedono hardware dedicato. NVIDIA Firewall, un firewall end-point, non supporta la funzionalità gateway a livello applicativo.

## Firewall come difesa dagli hacker (anti-hacking)

Un pacchetto IP “spoofed” è dotato di un valore generato illegalmente nel suo campo indirizzo sorgente IP. Utilizzando intenzionalmente un indirizzo IP errato, un hacker può creare diversi tipi di aggressione. La più famigerata è il cosiddetto attacco denial-of-service distribuito (DDoS), che è anche una delle aggressioni più comuni di chi si avvale dello spoofing IP. Queste aggressioni DDoS si fondano su due fattori: 1) un dispositivo “zombie” connesso a Internet, spesso un PC, che sia stato in qualche modo infiltrato; e 2) la possibilità di controllare il PC zombie in modo da inviare pacchetti con indirizzi di sorgente IP soggetti a spoofing.

I firewall sono sempre stati in grado di effettuare filtrature sulla base di indirizzi IP, ma il rilevamento di pacchetti con spoofing richiede una distinzione ben più sottile. Per esempio, sulla base dell’indirizzo di sorgente IP di un determinato pacchetto, questo sarà arrivato sull’interfaccia che lo ha ricevuto, date le informazioni in possesso del firewall sulla sua tabella di routing? Un dispositivo intermedio potrebbe non riuscire a rilevare con facilità lo spoofing di uno specifico pacchetto.

L’approccio migliore consiste alla prevenzione dello spoofing consiste nel blocco alla sorgente di simili pacchetti — il PC zombie. Incorporando la funzionalità antispoofing direttamente nell’infrastruttura hardware/software di networking del PC, si impedisce che questo possa utilizzare qualsiasi indirizzo IP diverso da quelli assegnati staticamente o dall’indirizzo assegnato mediante DHCP.

---

## Altre importanti funzioni di sicurezza

Il firewall fornisce un “livello” di protezione ed è solitamente considerato il livello base. Tuttavia, una soluzione di sicurezza davvero completa deve articolarsi su più livelli.

Queste funzionalità aggiuntive non sono fornite da NVIDIA Firewall, ma possono essere ottenute mediante la selezione dei migliori componenti in base ai requisiti definiti dall'utente.

## Protezione anti-intrusione

Il rilevamento delle intrusioni è la capacità di analisi di tutto il traffico in ingresso per individuare modelli di comportamento che corrispondono ad aggressioni di tipo noto o a precursori di questi attacchi. Per esempio, per aggredire una parte vulnerabile di un software applicativo di rete, l'aggressore potrebbe per prima cosa effettuare una scansione di tutte le porte possibili per cercare un esempio noto di una parte vulnerabile del software. Quindi, l'individuazione di una "scansione delle porte" può indicare che si sta per verificare un'aggressione e si possono quindi prendere misure difensive prima ancora di subire qualsiasi danno.

Grazie alla prevenzione delle intrusioni, comunque, vari attacchi noti vengono rilevati direttamente e battuti prima ancora che possano nuocere al sistema protetto.

In entrambi i casi, il software anti-intrusione dipende strettamente da informazioni contenute nella sua libreria di aggressioni note. Questi prodotti solitamente non sono in grado di rilevare i nuovi attacchi, perché non è ancora stata individuata la "firma" di quel tipo di aggressione.

## Protezione antivirus

Le capacità anti-virus proteggono il PC di un utente dall'esecuzione di codice che abbia virus o Trojan noti. Come nel caso dei prodotti anti-intrusione, le soluzioni anti-virus si basano su una libreria di aggressioni note, per le quali il prodotto attua misure difensive precise.

Inoltre, certi prodotti anti-virus possono avvisare gli utenti di eventuali attività sospette, anche se non sono in grado di abbinarle a un virus noto.

---

## NVIDIA Firewall

NVIDIA Firewall ora si basa sul motore di networking sicuro ActiveArmor, che lo rende il primo vero firewall per PC a base hardware del settore. Grazie a questo motore di networking sicuro, NVIDIA Firewall non grava sulla CPU per le attività di protezione.

La soluzione di networking sicuro NVIDIA ActiveArmor — una combinazione di NVIDIA Firewall e del motore sicuro ActiveArmor — migliora il throughput di rete a velocità gigabit Ethernet piene, riduce l'utilizzo della CPU, esegue ispezioni approfondite dei pacchetti e migliora la sicurezza di rete complessiva (figura 1).

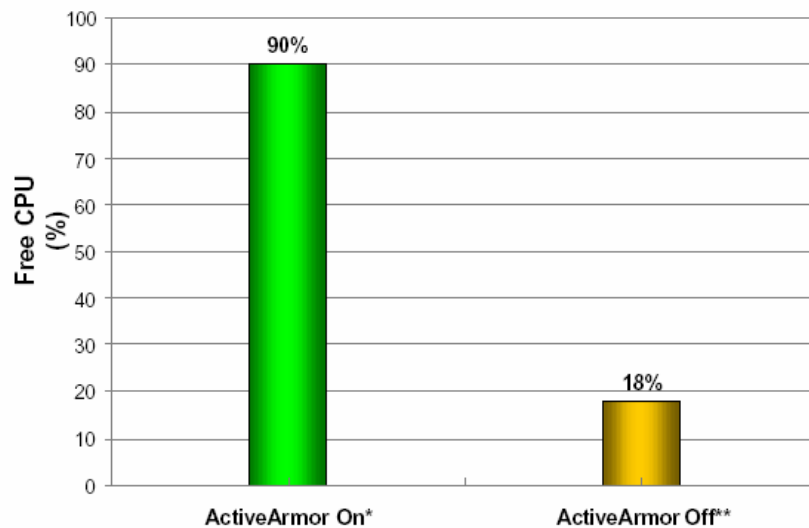


Figura 1. NVIDIA ActiveArmor offre il massimo delle prestazioni e il minimo utilizzo della CPU

**Note:**

NVIDIA Firewall incorpora sia le tecnologie firewall che quelle antihacking. Inoltre, la soluzione supporta l'ispezione stateless e stateful, la gestione basata sul Web, i profili di sicurezza predefiniti, la filtratura del blocco delle porte, Intelligent Application Manager, l'amministrazione remota e un Wizard di facile impiego. Oltre a ciò, NVIDIA Firewall dispone di funzionalità anti-hacking quali anti-IP-spoofing, anti-sniffing, anti-ARP-cache-poisoning e anti-DHCP server — importanti controlli di sicurezza per gli ambienti di rete aziendali.

In un ambiente aziendale, un firewall end-point (come ad esempio un firewall desktop) con capacità anti-hacking può ridurre le falle di sicurezza di origine interna e può impedire la generazione di traffico non autorizzato da parte dei desktop. Il risultato è un netto miglioramento della sicurezza generale, con requisiti ridotti da parte del personale IT.

## Funzionalità di gestione avanzata

NVIDIA Firewall offre numerose funzionalità di gestione avanzata quali accesso, configurazione e monitoraggio remoto, l'interfaccia riga di comando (CLI) e gli script WMI. Inoltre, è facile da utilizzare e configurare mediante un wizard intuitivo.

Queste funzionalità avanzate di gestione rendono NVIDIA Firewall particolarmente flessibile, facile da usare e molto potente (figura 2).

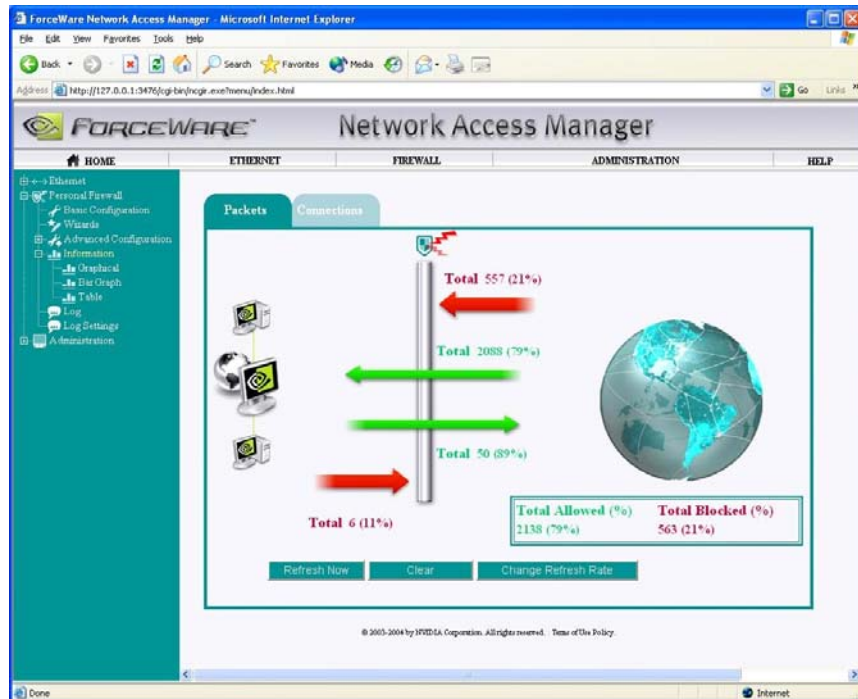


Figura 2. Configurazione semplificata grazie all'interfaccia browser basata sul Web

## Intelligent Application Manager (IAM)

Intelligent Application Manager è una funzione aggiuntiva di NVIDIA Firewall che integra il filtraggio basato sull'applicazione alla serie già estremamente completa di capacità firewall. IAM estende gli elementi di gestione della politica NVIDIA Firewall per fornire il filtraggio basato sulle applicazioni, sia che agiscano da client che da server. IAM include gli utenti nel percorso informativo/decisionale, consentendo loro di decidere quali elementi possano essere lasciati entrare senza pericolo e quali vadano esclusi dalla loro macchina. Una volta che un'applicazione è stata ammessa, questa può aprire le porte senza una configurazione specifica da parte dell'utente (figura 3).

IAM elimina la possibilità che un'applicazione canaglia residente nel PC dell'utente possa inviare traffico che sia riuscito a penetrare il firewall; il traffico in uscita viene ammesso soltanto se proviene da un'applicazione che l'utente ha definito come

sicura. IAM è persino in grado di verificare le applicazioni esistenti e di determinare se siano state alterate — per esempio, da un virus o da un Trojan integrati nell'eseguibile, o da un'applicazione che si è rinominata per imitarne una nota e sicura.

IAM è inoltre utile per la protezione del PC da pacchetti in entrata. Questa soluzione limita l'abilità dei Trojan o di altri Spyware di configurarsi come server per il PC, impedendo loro la ricezione di traffico dall'esterno del PC. Non solo IAM è in grado di filtrare i risultati sulla base delle porte, ma può anche proibire al server di aprire qualsiasi socket, impedendogli di ricevere traffico dal layer dell'applicazione.

IAM offre il massimo della protezione dalle aggressioni, proteggendo il PC dagli attacchi di entità esterne oltre a impedirgli di attaccare altri PC.

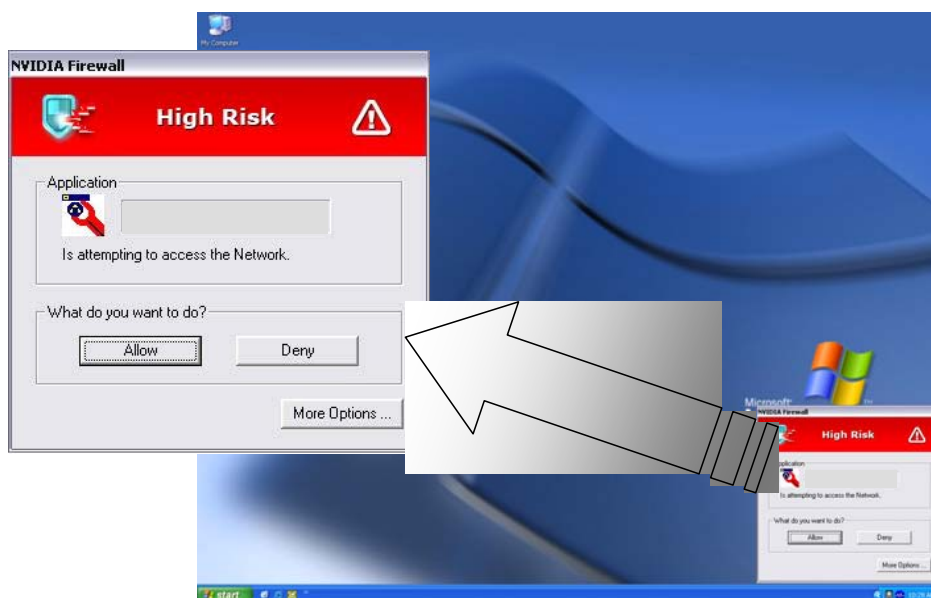



Figura 3. IAM avvisa quando applicazioni sconosciute tentano di accedere alla rete

## Perché scegliere NVIDIA Firewall?

La maggior parte dei firewall per PC sul mercato sono add-on a base software, mentre NVIDIA Firewall è il primo firewall per PC a base hardware del settore. Inoltre, la soluzione di networking sicuro NVIDIA ActiveArmor, che consiste di NVIDIA Firewall e del motore ActiveArmor, migliora la sicurezza complessiva della rete.



Oltre a ciò, NVIDIA Firewall presenta caratteristiche esclusive, quali ad esempio Intelligent Application Manager (IAM), la gestione avanzata — accesso, configurazione e monitoraggio remoto — e la massima facilità d'uso e configurazione grazie a un wizard semplice e intuitivo. Inoltre, questa soluzione può essere implementata in ambienti aziendali, che includono un firewall end-point (ad esempio i firewall per desktop). Oppure può essere utilizzato in ambienti domestici, ad esempio nei casi in cui un PC viene collegato a una connessione Internet a banda larga, per proteggere il PC da accessi non autorizzati.

La tecnologia NVIDIA Firewall può essere utilizzata come mezzo di attuazione di politiche di accesso e utilizzo, offrendo massima flessibilità e potenza straordinaria anche in questo ruolo. Per una protezione davvero completa, gli utenti dovrebbero integrare la protezione fornita da NVIDIA Firewall con le migliori applicazioni software anti-virus e anti-intrusione. A questo modo sarà possibile ottenere una soluzione di sicurezza PC davvero completa e inviolabile.



### **Notifica**

TUTTE LE SPECIFICHE DI PROGETTAZIONE NVIDIA, LE SCHEDE DI RIFERIMENTO, I FILE, I DISEGNI, LA DIAGNOSTICA, LE LISTE E ALTRI DOCUMENTI (UNITAMENTE E SEPARATAMENTE, DEFINITI "MATERIALI") SONO FORNITI NELLO STATO IN CUI SI TROVANO. NVIDIA NON OFFRE GARANZIE, ESPRESSE, IMPLICITE, STATUTARIE O DI ALTRO TIPO IN RELAZIONE AI MATERIALI, E RIFIUTA ESPRESSAMENTE OGNI GARANZIA IMPLICITA DI NON VIOLAZIONE, COMMERCIALIZZABILITÀ E IDONEITÀ A SCOPI SPECIFICI.

Le informazioni fornite sono ritenute accurate e affidabili. Tuttavia, NVIDIA Corporation non si assume alcuna responsabilità per le eventuali conseguenze derivanti dall'uso di tali informazioni o da qualsiasi violazione di brevetti o altri diritti di terze parti che possono conseguire dal loro uso. Non viene concessa alcuna licenza implicita o in altro modo in base a nessun brevetto o diritto di autore di proprietà di NVIDIA Corporation. Le specifiche tecniche menzionate nella presente pubblicazione sono soggette a modifica senza preavviso. Questa pubblicazione rimpiazza e sostituisce tutte le informazioni precedentemente fornite. Non si autorizza l'impiego dei prodotti di NVIDIA Corporation come componenti cruciali di dispositivi per il supporto vitale o per sistemi che non abbiano ricevuto l'espressa approvazione scritta di NVIDIA Corporation.

### **Marchi**

NVIDIA, il logo NVIDIA e ActiveArmor sono marchi registrati o marchi di NVIDIA Corporation negli Stati Uniti e in altri paesi. Altri nomi di società e di prodotti possono essere marchi o marchi registrati dei rispettivi detentori.

### **Copyright**

© 2004 by NVIDIA Corporation. Tutti i diritti riservati.



**NVIDIA.**

NVIDIA Corporation  
2701 San Tomas Expressway  
Santa Clara, CA 95050  
[www.nvidia.com](http://www.nvidia.com)