NORMAN®

Application and Device Control

FUNZIONI PRINCIPALI

Whitelist / Rifiuto predefinito

Crittografia basata su criteri e limitazione della copia dei dati per gli archivi rimovibili

Filtro per tipo di file

Accesso temporaneo / programmato

Autorizzazioni in base al contesto

Ruoli centralizzati di gestione / amministrazione

Controllo accessi in base al ruolo

Agente a prova di manomissione

Architettura flessibile e scalabile

Individuazione automatica delle applicazioni

Definizioni standard dei file

Autorizzazione automatica degli aggiornamenti software

Protezione di script e macro

Autorizzazione flessibile dei file

Autorizzazione locale

Controlli distribuiti

Protezione del computer offline

Active Directory e eDirectory Support

Protezione proattiva degli endpoint per creare un ambiente applicativo sicuro

Con l'emergenza della tecnologia consumer, i social network, le tecnologie Web 2.0 e i cybercriminali sempre più sofisticati, la protezione degli endpoint è diventata una lotta continua.
Norman Application and Device Control impedisce agli endpoint di diventare la porta di accesso per i rischi alla sicurezza che possono infiltrarsi e causare la fuga dei dati riservati; inoltre, rappresenta un modo efficace per creare un ambiente sicuro e produttivo.

Motivazioni e problematiche aziendali

Nel contesto economico attuale, trovare un punto di equilibrio tra la semplicità del business e la protezione degli endpoint non è facile.Gli endpoint non sono più scrivanie degli uffici in un ambiente controllato.I dipendenti installano applicazioni illecite e non autorizzate sui computer fissi e portatili, causando l'aumento delle chiamate di assistenza, problemi di prestazioni e tempi di inattività.

In più, la minaccia dei malware è in aumento.Gli analisti stimano che il 75% delle organizzazioni sia stato colpito da malware mirati e spinti da motivazioni finanziarie, in grado di superare le barriere tradizionali e le difese degli host1.Da uno studio condotto recentemente è risultato che la presenza dei malware è cresciuta di oltre il 500%, con più di 5,49 milioni di campioni distinti di software dannosi segnalati2.Come se ciò non bastasse, gli attacchi stanno diventando sempre più mirati e studiati appositamente per raggirare le soluzioni antivirus.

Una protezione efficace degli endpoint richiede un approccio proattivo e sufficientemente flessibile da bilanciare la produttività degli utenti e le esigenze di sicurezza aziendale.

Protezione degli endpoint aziendali da malware e software non autorizzati

Norman Application and Device Control offre la protezione completa degli endpoint da malware e minacce sconosciute, spingendo allo stesso tempo all'utilizzo dei software autorizzati.Norman Application Control, il componente principale di questa soluzione, consente di gestire, monitorare e controllare centralmente le applicazioni.Con un metodo basato sul whitelisting delle applicazioni, è possibile fare in modo che soltanto le applicazioni autorizzate vengano eseguite su computer portatili, fissi, server mission critical e terminali POS, impedendo l'esecuzione di codici dannosi o sconosciuti.

I malware infettano i sistemi in pochi secondi, molto meno del tempo impiegato dai produttori di antivirus per rilasciare firme.I server mission-critical devono essere disponibili 24/7.Grazie al whitelisting delle applicazioni, sui server vengono eseguite soltanto le applicazioni autorizzate, escludendo le minacce.

Inoltre è possibile migliorare la gestione operativa di desktop e server eliminando le chiamate di supporto superflue e i problemi di prestazioni derivanti dall'impiego di software illeciti o non autorizzati.Sarà più facile dimostrare la conformità individuando tutte le applicazioni in uso nell'ambiente, applicando criteri di licenza del software e creando un audit trail dettagliato di tutti i tentativi di esecuzione delle applicazioni.

[1] Gartner Research, Gartner's Top Predictions for IT Organizations and Users, 2007 and Beyond, Daryl C. Plummer, December 1, 2006

[2] www.AVtest.org, 2008

Ha detto un utente: “È un immenso sollievo sapere che, quando forniamo ai dipendenti un computer, questo continuerà a rimanere così come lo abbiamo configurato.”

Ha detto un utente: “Offre una visione unitaria e semplice su tutti i programmi che accedono o tentano di accedere alla rete attraverso gli endpoint aziendali, dalla prospettiva dei dispositivi e delle applicazioni con un nuovo livello di visibilità nella rete che prima non era possibile.”

Come funziona Norman Application and Device Control:

1. *Individuazione:identifica tutti i file eseguibili, raccoglie profili e li organizza in gruppi di file predefiniti.*
2. *Implementazione:concede autorizzazioni per l’esecuzione delle applicazioni in base agli attributi eseguibili, utente o gruppo utenti.Il whitelisting delle applicazioni garantisce che sui computer vengano eseguite soltanto le applicazioni autorizzate e lecite.*
3. *Controllo:controlla l’efficacia dei criteri di protezione degli endpoint in tempo reale e identifica le potenziali minacce registrando tutti i tentativi di esecuzione delle applicazioni e tenendo traccia di tutte le modifiche dei criteri e delle attività dell’amministratore.*
4. *Report:dimostra l’ottemperanza ai criteri e garantisce la conformità alle licenze software tramite il drill down dei comportamenti sospetti per azioni legali o di sicurezza.*

Principali vantaggi

- Determina automaticamente quali applicazioni vengono utilizzate nell’organizzazione.
- Definisce i criteri di sicurezza in base a regole globali e specifiche per l’utente e/o per la macchina, a seconda delle esigenze aziendali, tramite un metodo di “whitelisting”.
- Fa rispettare i criteri di utilizzo delle applicazioni in tutta la rete.
- Registra automaticamente gli eventi di rete relativi ai criteri di sicurezza degli endpoint.
- Offre il controllo e l’esecuzione a livello aziendale in base a un’architettura scalabile client-server con un database centralizzato che semplifica il bilanciamento del carico e il controllo distribuito.
- Installa agenti a prova di manomissione su ogni endpoint della rete e ne impedisce la rimozione non autorizzata.
- Supporta completamente la struttura Windows Active Directory e Novell eDirectory / NDS.

Principali vantaggi

- Automatizza l’applicazione delle misure di sicurezza
- Consente di risparmiare tempo e migliora la gestione dei desktop e del server
- Fa rispettare la conformità nell’organizzazione
- Si adatta all’evoluzione dell’azienda

REQUISITI DI SISTEMA

Server: Windows Server 2003 & 2008

Client: Windows XP Professional, Windows 2000 Professional, Windows Server 2003, Windows Vista

SAND BOX · D N A MATCHING · STATIS-TICS · UPDATE · UNREAD MAIL · SECURED · VIRUS SCAN · DOCU-MENTS

Norman ASA è leader mondiale nel campo della sicurezza dei dati, protezione Internet e tool di analisi. Grazie alla tecnologia proprietaria SandBox, Norman è in grado di offrire una protezione proattiva unica rispetto ad ogni altro concorrente. Attraverso il focus su tale tecnologia, l’azienda ha stretto alleanze che consentono a Norman di offrire un range completo di servizi nel campo della sicurezza IT. Norman è stata fondata nel 1984, il quartier generale è in Norvegia e i mercati di riferimento sono l’Eruopa continentale, il Regno Unito e gli USA.

NORMAN®