

Analisi del comportamento dell'utente: visibilità conveniente in tempo reale dell'attività degli utenti sulla rete aziendale



Executive Summary

La maggior parte delle aziende sono accomunate da esigenze reali di business e requisiti di conformità che vanno costantemente monitorati e verificati:

- Chi accede ai sistemi di business critici?
- Cosa utilizzano tali utenti?
- In quale parte della rete stanno svolgendo delle attività?

Per ridurre in modo efficiente i rischi all'interno della rete e soddisfare i requisiti di conformità, è fondamentale disporre di visibilità costante sulla rete e sulle applicazioni di business critiche. La parte difficile è che, quando si cerca di ottenerla in modo manuale, tale visibilità non offre niente più che un' "istantanea del momento" statica dopo che si è verificato l'evento, ovvero non in tempo reale. Non è assolutamente in grado di fornire una visione costante, precisa e conveniente dell'accesso e del comportamento di un utente.

Questa mancanza di visibilità e, di conseguenza, di supporto per le decisioni mette in difficoltà i dipartimenti IT e di sicurezza ogni volta che le minacce colpiscono l'azienda. Tale mancanza di visibilità, inoltre, porta frequentemente a attività di verifica relativamente a:

- Lacune nel dimostrare ininterrottamente la verifica dell'accesso di terze parti
- Lacune nel monitoraggio costante di condizioni limite come separazione delle mansioni e leggi internazionali sulla privacy
- Lacune nel monitoraggio dell'accesso utente privilegiato

Panoramica di McAfee Network User Behavior Monitor

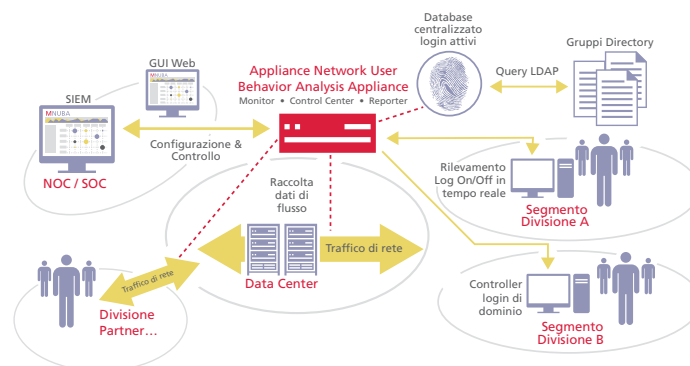
Per risolvere tali sfide, McAfee Network User Behavior Monitoring (Network UBA) (Securify) fornisce monitoraggio automatico basato sull'identità per mantenere l'azienda conforme e sotto controllo. Questa soluzione completa di monitoraggio offre visibilità completa e verifica di chi fa cosa e dove in tempo reale, automaticamente e costantemente. Con identità, intendiamo il nome utente effettivo, nome del gruppo e ruolo correlati al comportamento e forniti in tempo reale, non dopo che si è verificato il fatto. Le nostre soluzioni di rete fuori banda non richiedono agent endpoint o ricodifica di applicazioni personalizzate, e possono essere implementate e rese operative in poche ore.



La vista Discovery (Individuazione) offre alle aziende una comprensione iniziale di quali gruppi utente accedono a quali sistemi critici. Tale visibilità permette di risparmiare una quantità di tempo considerevole nell'acquisizione di informazioni sull'utilizzo dei sistemi da parte di utenti, protocolli/servizi, larghezza di banda, ecc.



Utilizzando controlli basati su ruoli, la vista Control (Controllo) illustra graficamente l'utilizzo di rete degli utenti dei sistemi critici e denota chiaramente quali attività sono accettabili, non accettabili e quale attività richiede un'analisi più approfondita dai gruppi di sicurezza e operation.



Una soluzione McAfee Network UBA rappresentativa implementata davanti a un data center che ospita sistemi di business critici.

Panoramica sulla soluzione

Analisi del comportamento dell'utente:
visibilità conveniente in tempo reale
dell'attività degli utenti sulla rete aziendale

Le funzionalità di McAfee Network UBA

Monitoraggio e analisi della rete

- Monitoraggio tramite mirroring delle porte o tap di rete passivi per un'approfondita ispezione dei pacchetti
- Monitoraggio tramite dati di flusso di Cisco Netflow, Juniper J-Flow e altri

Funzionalità di rilevamento

- Rilevamento scansioni di rete
- Rilevamento service probe
- Rilevamento anomalie di protocollo
- Rilevamento anomalie del comportamento di rete
- Rilevamento anomalie del comportamento delle applicazioni
- Rilevamento servizi non autorizzati
- Rilevamento canali di comunicazione non autorizzati
- Rilevamento signature IDS native:
 - » Implementazione signature personalizzate
 - » Aggiornamenti di signature regolari e on-demand

Funzionalità relative all'identità

- Tracciamento dell'identità dell'utente tramite integrazione in tempo reale con l'infrastruttura di directory esistente
- Sfruttamento di contesti esistenti di utente, ruolo e policy
- Tracciamento dell'attività complessiva dell'utente dal momento in cui l'utente accede alla rete
- Polling costante e non invasivo delle directory
- Spostamenti, aggiunte e modifiche effettuati una volta nella directory, che poi filtra ai Monitor Network UBA
- Controlli basati su identità, gruppo e ruolo:
 - » Granularità del controllo: gruppi utente rispetto ai segmenti di rete
 - » Controlli espressi in contesti di business semplici da comprendere
 - » Supporto di ambienti tipici DHCP con gruppi di indirizzi casuali

Integrazione

- Integrazione con directory come Microsoft Active Directory e directory LDAP
- Integrazione con router di rete e switch per bloccare le azioni
- Integrazione con dati basati su flusso da Cisco, Juniper e altri
- Invio di avvisi sugli eventi al security information manager (SIM) e ad altri sistemi di terze parti come ArcSight tramite:
 - » SNMP
 - » SMTP
- Integrazione con clienti non-Windows basati sull'identità come Centrify
- Importazione delle valutazioni delle vulnerabilità

Sostanzialmente, le aziende calcolano il valore offerto da McAfee Network UBA attraverso una combinazione di:

- Riduzione del rischio posto dagli insider
- Miglioramento significativo dell'efficienza attraverso la visibilità sulla rete
- Metriche costanti di conformità

La principale sfida per le aziende: mancanza di visibilità sulla rete

In base a stime McAfee, derivate da colloqui con decine di aziende Fortune 500, fino al 70% dei progetti attuali richiede attività manuali di discovery e analisi per stabilire chi fa cosa sulla rete e dove. Inoltre, processi manuali come analisi dei log, indagini e altre attività sono storicamente imprecisi e richiedono molto lavoro. Di conseguenza, vengono effettuati raramente. Anche quando le aziende riescono ad ottenere visibilità, non sono in grado di visualizzare e verificare costantemente chi è sulla rete, da dove proviene, dove è diretto e cosa fa ogni singolo utente una volta arrivato a destinazione.

Di seguito esamineremo i requisiti di visibilità e verifica per le tre principali iniziative IT.

Sfida: Visibilità limitata su chi sta facendo cosa e dove sui sistemi di business critici (rischio degli insider)

Pratiche pericolose e improprie da parte di "insider" autorizzati possono creare un rischio sostanziale per i sistemi di business critici. Personale in outsourcing, sviluppatori offshore, collaboratori, dipendenti irresponsabili, partner, joint venture, ecc. devono essere monitorati. Ancora, è praticamente impossibile monitorare in tempo reale la sicurezza in base agli standard raccomandati dal CERT ed altri enti utilizzando gli strumenti di sicurezza tradizionali. Inoltre, l'utilizzo di dati di log per ottenere questo livello di informazioni può "consumare" preziose risorse IT, continuando a non fornire visibilità operativa e controllo in tempo reale.

McAfee Network UBA fornisce visibilità costante in tempo reale attraverso il monitoraggio di "chi, cosa e dove" sulla rete per prevenire rischi e minacce. Nello specifico, Network UBA permette di:

- Utilizzare elenchi di controllo per monitorare utenti ad alto rischio in tempo reale e ricevere allarmi su abusi, come leap-frogging o outsourcing non autorizzato, su misura per l'ambiente di business specifico dell'azienda
- Rilevare comportamenti anomali, non protetti e pericolosi da parte di personale in outsourcing e utenti privilegiati in tempo reale
- Rilevare attività indicative di abusi di rete, come scansioni di rete, service probe, login falliti e propagazione di worm
- Rilevare quando gli utenti superano le soglie stabilite in termini di larghezza di banda di rete, tempo del sistema e altre risorse per ogni utente
- Fornire informazioni sul contesto di rete per rilevare fonti non autorizzate e superare i sistemi d'accesso
- Risolvere i problemi in implementazioni di controllo dell'accesso alla rete (NAC) e monitoraggio e filtering dei contenuti (CMF) verificando tutto il traffico relativo, anche se mascherato
- Monitorare i sistemi che contengono informazioni di identificazione personale (PII)
- Proteggere i sistemi critici
- Collegare in modo sicuro e monitorare le reti di partner e alleati di coalizioni militari
- Ridurre vulnerabilità e rischi associati al passaggio da IPv4 a IPv6

Sfida: Una visibilità limitata aumenta il carico di lavoro in modo considerevole durante modifiche all'infrastruttura e operazioni di rete costanti

Che si tratti di una fusione o di un'acquisizione, o di una segmentazione di rete, virtualizzazione o consolidamento, le aziende hanno bisogno di avere visibilità su chi sta facendo cosa sulla rete e dove, prima durante e dopo modifiche complesse all'infrastruttura. Inoltre, il livello di visibilità necessita di processi manuali che richiedono molto tempo e risorse.

McAfee Network UBA supporta l'azienda con:

- Ampia visibilità conveniente sullo stato puntuale della rete per il consolidamento di rete e data center e migrazione delle reti legacy, tra cui:
 - » Utilizzo delle applicazioni per collegare e consolidare i sistemi
 - » Utilizzo di applicazioni e porte per garantire la compatibilità del sistema
 - » Utilizzo del sistema per consolidamenti e decommissioning

Panoramica sulla soluzione

Analisi del comportamento dell'utente:
visibilità conveniente in tempo reale
dell'attività degli utenti sulla rete aziendale

Le funzionalità di McAfee Network UBA - continua

Decodifica dell'applicazione

- Cattura e decodifica dei pacchetti a livello di comando per 20 applicazioni principali, tra cui: DHCP, AIM, DNS, FTP, HTTP, IRC, Kerberos, POP, SIP, SMTP, SSL, TLS, YIM e altro

Certificazione

- Certificazione Common Criteria EAL 3
- Accredamenti del Dipartimento della Difesa degli Stati Uniti per l'operatività con SIPRNet, NIPRNet e JWICS

Controlli

- Oltre 300 controlli precostituiti per il comportamento di rete e applicazioni:
 - » Include controlli di URL e velocità
 - » Interfaccia basata su wizard per stabilire controlli e gruppi di controllo e semplice funzione di creazione di controlli personalizzabili
 - » Soglie a livello di applicazione definite dall'utente per numero di eventi e larghezza di banda per giorno e ora
 - » HT definito dall'utente

- » Conformità di rete e applicazioni alle best practice di sicurezza
- » Status di migrazione dell'utente
- Migliore utilizzo della larghezza di banda
- Una visione intuitiva in tempo reale del traffico di rete per porre rimedio a configurazioni errate di firewall, router e altri dispositivi

Sfida: Riduzione di costi e attività per la conformità con le normative e preparazione a processi di audit

La mancanza di visibilità di cui abbiamo discusso precedentemente è anche parzialmente responsabile dei costi elevati e degli sforzi supplementari associati alle verifiche IT. Queste verifiche sono tipicamente guidate da risultati di audit che evidenziano mancanze nei controlli preventivi esistenti, che sono molto più difficili da risolvere durante e dopo le verifiche.

McAfee Network UBA aiuta a semplificare le normali verifiche IT e consente di prepararsi ai processi di verifica. E' anche utile per garantire la conformità con le normative e prevenire eventuali risultati di verifica colmando le lacune nei controlli preventivi esistenti. McAfee Network UBA è più apprezzato da aziende che sono regolamentate da due o più normative, tra cui Sarbanes Oakley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Payment Card Industry (PCI) e altre normative federali e statali.

McAfee Network UBA aiuta ad affrontare in modo proattivo verifiche IT periodiche, riduce il tempo di preparazione alle verifiche e migliora la posizione in caso di verifica fornendo:

- Monitoraggio per verifica e conformità
- Verifica dell'accesso reale per utenti, gruppi e ruoli per garantire l'efficacia dei controlli d'accesso
- Monitoraggio e reporting di conformità più semplici
- Miglioramento della posizione in caso di verifica grazie al rilevamento di utenti non autenticati e applicazioni non approvate, e disattivazione degli utenti o di privilegi su applicazioni commerciali non integrate
- Verifica dell'accesso di utenti con privilegi con ampi diritti, come lo staff IT in outsourcing
- Prove migliori per i revisori, come verifica dell'accesso, gestione della configurazione e altro
- Verifica dell'accesso dopo l'implementazione di un sistema di controllo logico degli accessi per soddisfare la direttiva HSPD-12
- Identificazione delle risorse e dei punti d'accesso della rete
- Monitoraggio costante per garantire la conformità con PCI, SOX, FISMA e altre normative

Le sfide con le soluzioni esistenti: Visibilità manuale limitata e dispendiosa in termini di tempo

Si potrebbero utilizzare varie soluzioni singole e processi manuali per ottenere il livello di visibilità e verifica richiesto per ogni iniziativa IT nella sezione precedente. Comunque, il costo e l'impegno di tale tentativo sono proibitivi, e per gruppi IT a corto di risorse, non realistici.

La seguente tabella fornisce una breve panoramica delle soluzioni tipiche utilizzate per ottenere visibilità e alcune delle sfide nell'utilizzo di tali soluzioni:

Metodo o soluzione esistente	Le sfide
Indagini e sondaggi manuali	Indagini e sondaggi manuali sono una parte intrinseca del far funzionare una rete. Comunque, quando utilizzati per una visibilità in tempo reale, non sono efficaci. A causa di varie fonti e errori umani, sono imprecisi. Sono inoltre inefficaci e dispendiosi in termini di tempo.
Strumenti Security Information/Event Management (SIEM) e di raccolta dei log	Gli strumenti SIEM risultano validi tanto quanto gli elementi basilari che pre-elaborano i dati e inviano allarmi alla console SIEM. Le soluzioni SIEM e di gestione dei log elaborano inoltre le informazioni disponibili dai log di applicazioni e database. Ma il loro focus primario è la raccolta di dati per un'analisi forensica post-evento. Gli strumenti SIEM non forniscono visibilità o verifica in tempo reale.
Network Behavior Analysis (NBA)	Utilizzata per esaminare impieghi anomali della rete, la tecnica NBA tipicamente richiede l'impostazione di una linea di base. Ciò risulta piuttosto difficile, senza creare troppo disturbo, in un ambiente dinamico. Inoltre, gli strumenti NBA tipicamente non analizzano in modo approfondito le transazioni delle applicazioni, come HTTP Get rispetto a HTTP Put, o dati delle applicazioni, come il contenuto del campo URL. Inoltre, tipicamente non legano il nome utente reale, nome di gruppo e ruolo a un'attività per offrire una visibilità proattiva in tempo reale.
Controllo di accesso alla rete (NAC)	Sebbene NAC sia perfetto per evitare che host compromessi si colleghino alla rete aziendale e verificare gli host per la postura complessiva di sicurezza, si dimostra limitato nella sua capacità di tracciare l'attività post-accesso. L'approccio che fornisce un'istantanea statica non monitora né impone attività conseguenti da parte di quell'host una volta ottenuto l'accesso.

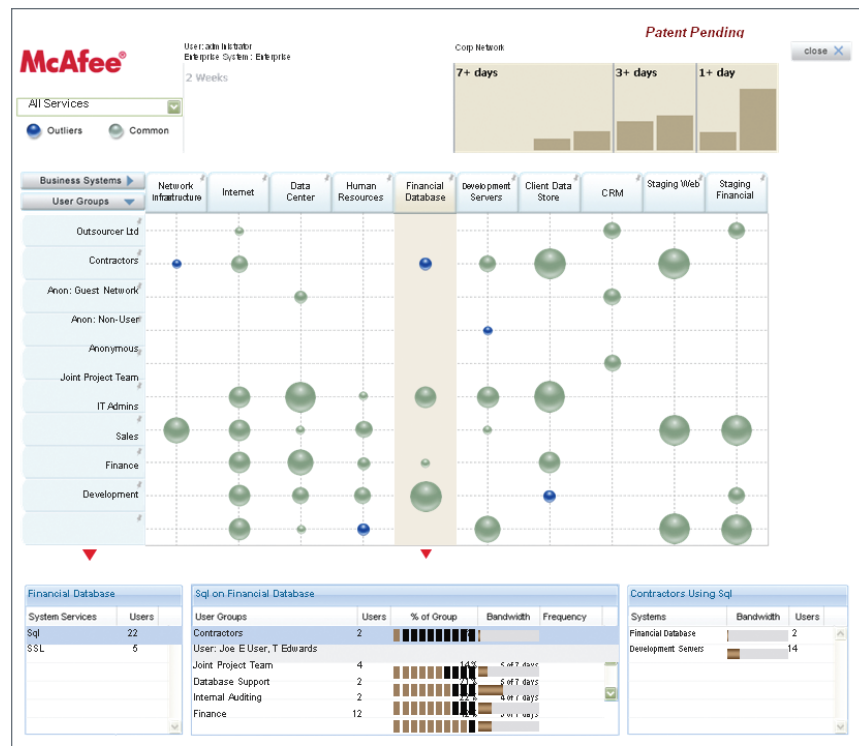
Panoramica sulla soluzione

Analisi del comportamento dell'utente:
visibilità conveniente in tempo reale
dell'attività degli utenti sulla rete aziendale

Funzionalità esclusiva: Discovery automatica

La funzionalità di discovery automatica di McAfee Network UBA aiuta a scoprire il "chi, cosa e dove" durante la fase di pianificazione dei progetti di cambiamento, senza richiedere la definizione di alcuna regola. La Discovery Dashboard della soluzione fornisce una visione unica del traffico monitorato passivamente e correla i gruppi utente e la loro attività associata su sistemi di business critici. Le appliance McAfee Network UBA non richiedono agent e comunicano direttamente con le directory esistenti, sfruttando gruppi e iscritti esistenti. (Gruppi su misura possono essere aggiunti se necessario.)

McAfee Network UBA fornisce inoltre funzionalità aggiuntive di analisi, inclusa la capacità di focalizzarsi su un unico sistema. Per esempio, si potrebbe concentrare Network UBA su un CRM specifico o un sistema di contabilità. Allo stesso modo, si può utilizzare Network UBA per individuare tutti i gruppi utente o focalizzarsi su un gruppo utente specifico, posizione dell'ufficio o confine della rete. Per esempio, si potrebbero monitorare i rappresentanti commerciali che accedono a un particolare sistema dalla sede centrale. Vengono inoltre fornite informazioni aggiuntive su cosa stanno facendo gli utenti, inclusi decodifica dei protocolli, porte, larghezza di banda, URL e comandi. Questo livello di dettaglio è estremamente utile per attività di rezoning e segmentazione di rete, o spostamenti di applicazione e server che potrebbero influenzare la capacità degli utenti di accedere alle applicazioni.



La vista Discovery (Individuazione) di Network UBA fornisce una rappresentazione grafica iniziale alle aziende di quali utenti e gruppi stanno accedendo a quali sistemi critici (automaticamente, senza richiedere una linea di base statica). Tale visibilità permette di risparmiare una quantità di tempo considerevole nell'acquisizione di informazioni sull'utilizzo dei sistemi da parte di utenti, protocolli/servizi, larghezza di banda, ecc.

Funzionalità esclusiva: Verifica automatica

La funzionalità di accertamento di McAfee Network UBA si sviluppa sulla visione di discovery. La funzione di accertamento di McAfee Network UBA verifica il traffico rispetto a controlli basati su ruoli e best practice di sicurezza pre-costruite. McAfee Network UBA offre oltre 300 controlli pre-costruiti e personalizzabili per verificare cosa fanno gli utenti dopo aver ottenuto accesso alla rete. Le appliance McAfee Network UBA non richiedono agent e comunicano direttamente con le directory esistenti, sfruttando gruppi e iscritti esistenti. (Se necessario, possono essere aggiunti gruppi su misura.)

Panoramica sulla soluzione

Analisi del comportamento dell'utente:
visibilità conveniente in tempo reale
dell'attività degli utenti sulla rete aziendale

Funzionalità esclusiva: Identità basate su nome, gruppo e ruolo reali dell'utente

McAfee Network UBA si integra perfettamente con gli archivi directory esistenti, come Microsoft Active Directory, sfruttando informazioni su utente, gruppo e ruolo effettivi per stabilire dinamicamente quando un utente accede alla rete. McAfee Network UBA interroga la directory in tempo reale, e quindi mette in relazione gli utenti e loro gruppi con tutti gli accessi e attività correlati. Sottolineiamo che le credenziali d'identità dell'utente vengono rilevate all'interno del traffico da McAfee Network UBA senza l'utilizzo di alcun agent lato client o server.

Di seguito un esempio di McAfee Network UBA in azione. Un utente denominato jsmith si collega alla rete. McAfee identifica tale azione e stabilisce immediatamente che jsmith fa parte del gruppo marketing e ha un ruolo che le consente di accedere al database marketing e a un database di joint-venture ma non a quello finanziario. McAfee Network UBA continua a monitorare il traffico di rete per garantire che le azioni di jsmith rispettino tale policy oltre a tutte le altre stabilite dai controlli di sicurezza.



Applicando policy basate sugli utenti, la vista Control (Controllo) di Network UBA illustra graficamente l'utilizzo di rete degli utenti dei sistemi critici e denota chiaramente quali attività sono accettabili, non accettabili e quale attività richiede un'analisi più approfondita da parte dei gruppi di sicurezza e operation.

La funzionalità di accertamento di McAfee Network UBA può immediatamente definire e fornire avvisi in tempo reale relativamente ai seguenti esempi rappresentativi:

- Accesso da parte di utenti che non si autenticano, come dipendenti licenziati i cui privilegi d'accesso sono stati revocati
- Eccezioni all'accesso di rete come stampanti che non si comportano come previsto
- Verifica dell'accesso degli utenti che dovrebbero essere sulla rete, come dipendenti riassegnati o personale in outsourcing che hanno avuto accesso ai sistemi in modo inappropriato, forse involontariamente, cui non avrebbero dovuto
- Attività non garantite o pericolose, incluso tunneling di servizi come FTP all'interno di HTTP verso firewall di transito
- Verifica dell'utilizzo previsto di protocolli o comandi amministrativi, come l'autoring web

Come viene implementato McAfee Network UBA

McAfee Network UBA offre un'architettura a più livelli che include McAfee Network UBA Monitors, appliance McAfee Network UBA Control Center e appliance McAfee Network UBA Reporter. La nostra soluzione offre i vantaggi, in termini di implementazione, di una soluzione di rete fuori banda senza l'esigenza di integrare agent o applicazioni, ed è collaudata su reti mondiali estremamente sensibili, monitorando centinaia di migliaia di utenti per un singolo cliente e oltre 3 milioni di utenti in tempo reale per tutti i clienti.

Panoramica delle appliance McAfee Network UBA Monitor

Le appliance McAfee Network UBA Monitor rappresentano il caposaldo della soluzione complessiva McAfee Network UBA. I Monitor si basano su rete e sono studiati per acquisire e analizzare dati critici sul traffico all'interno della rete utilizzando uno dei tre seguenti metodi:

- I Monitor possono acquisire passivamente, decodificare e analizzare il traffico tramite un'analisi approfondita dei pacchetti nativa (Deep Packet Inspection - DPI). Utilizzano port mirroring o tap di rete passivi per ottenere dati complessivi di pacchetto per la decodifica dei protocolli fino al livello applicativo (layer 7). Questo livello di dettaglio è spesso necessario per garantire una visione a prova di manomissione dell'attività di rete all'interno di data center e sistemi di business critici.

Panoramica sulla soluzione

Analisi del comportamento dell'utente:
visibilità conveniente in tempo reale
dell'attività degli utenti sulla rete aziendale

- I Flow Monitor possono sfruttare i dati esistenti basati sul flusso da Cisco Netflow, Juniper J-Flow e altri per l'analisi. Questa visione di rete più ampia è spesso utile per ottenere una visione conveniente per l'intera azienda su chi sta facendo cosa e da dove sull'intera rete, incluse sedi remote.
- Quando si utilizzano appliance di gestione McAfee Network UBA, si possono utilizzare i Monitor in modalità "Mixed" (Mista) che combina dati sia DPI che basati su flusso.

Panoramica delle appliance McAfee Network UBA Reporter

Network UBA Monitors può effettuare un'analisi su base distribuita. Comunque, per report su termini più lunghi, le appliance McAfee Network UBA Reporter possono fornire un datawarehouse per acquisire e interrogare i dati per un periodo fino a un anno. Le appliance Network UBA Reporter offrono inoltre report pre-costituiti per la conformità e attività di forensics.

Panoramica delle appliance McAfee Network UBA Control Center

Per implementazioni con più Monitor, è possibile consolidare le informazioni utilizzando McAfee Network UBA Control Center. McAfee Network UBA può inoltre inviare allarmi SNMP automatici prioritizzati a sistemi di trouble ticket e personale di incident response quando necessario.

Questa ricca architettura accelera l'implementazione, scala per le aziende di più grandi dimensioni, e non richiede Monitor su sedi distribuite dell'utente, come divisioni o filiali, in modo da monitorare l'attività di rete.

Sommario

Le soluzioni identity-aware di McAfee Network UBA consentono di ridurre i costi e velocizzare l'implementazione della visibilità su "chi sta facendo cosa e dove" con le applicazioni e sulle reti. Oltre 60 aziende globali e importanti agenzie federali si affidano a McAfee Network UBA per aiutare a migliorare la visibilità sulla rete e l'analisi comportamentale di oltre 3 milioni di utenti.

In definitiva, le nostre soluzioni aiutano.

Miglioramento di efficienza e conformità

- Sostituzione di indagini manuali di discovery, che richiedono tempi lunghi
- Eliminazione delle attività manuali imprecise di verifica dei log
- Riduzione del tempo dedicato alle indagini relative a violazioni di accesso con dati correlati
- Minori disagi causati da modifiche errate ad infrastruttura e accesso
- Riduzione del tempo e degli sforzi per la ricodifica delle applicazioni

Riduzione del rischio

- Rilevamento di comportamenti inappropriati dell'utente dopo l'accesso
- Evita che gateway di sicurezza e controlli in accesso vengano aggirati
- Controbilanciamento del controllo per le applicazioni personalizzate non protette
- Rilevamento degli abusi di utenti disabilitati e riassegnati a nuovi ruoli
- Monitoraggio dell'utilizzo di account privilegiati

