White paper

Integrazione di sistemi host con framework di sicurezza moderni

Il mondo dei sistemi host è cambiato. Oggi, questi pilastri fondamentali delle aziende (ricchi di dati decennali) non si adattano ai vostri moderni framework di sicurezza. Infatti, il moderno framework di sicurezza protegge tutto, tranne gli host critici. Inoltre, nel frattempo, i requisiti normativi richiedono una protezione dei dati identica per tutto.

Questo white paper rivela un modo pratico per tenere al sicuro i vostri sistemi host, colmando il divario tecnologico, senza compromettere le attività aziendali.

opentext™

Sommario

pagina

L'host funziona in modo autonomo

Una volta, i sistemi host vivevano in un mondo sicuro. I dati host viaggiavano su un percorso protetto da e verso un terminale attendibile. L'host sapeva chi era l'utente, da dove provenivano i dati e dove andavano.

I tempi sono cambiati. Oggi, abbiamo reti aperte, architetture orientate ai servizi e hacker che attaccano più velocemente di quanto gli addetti IT possano reagire. La sicurezza dell'host non ha tenuto il passo. La tradizionale sicurezza dell'accesso host lascia i dati pericolosamente esposti in vari modi:

Autenticazione debole e decentralizzata

Tra un hacker malintenzionato e i vostri dati host critici potrebbe esserci solamente una password di otto caratteri. L'autenticazione basata su host, di per sé, non è in grado di sfruttare appieno la potenza del sistema di gestione delle identità utilizzato dal resto dell'azienda.

Autorizzazione debole e decentralizzata

Una volta connesso alla rete aziendale, un utente ha facile accesso alle vostre applicazioni host. Ciò significa che a un utente malintenzionato basta solo rubare le credenziali host di otto caratteri di un utente per accedere ai campi contenenti i dati personali.

Controllo decentralizzato

Il controllo dell'accesso viene eseguito da ciascun host in base all'ID host dell'utente. Quando sono coinvolti più host, gli amministratori della sicurezza devono esaminare i log su ognuno di essi, confrontando l'ID utente per ogni host con l'ID utente per l'azienda, per poter creare un audit trail completo.

Crittografia problematica

Fino all'arrivo della crittografia SSL/TLS, negli anni novanta, i dati e le password viaggiavano tra il client e l'host sotto forma di testo non cifrato. Non vi era alcun luogo sicuro, al riparo da occhi indiscreti. Lo standard SSL/TLS ha risolto il problema della crittografia, ma non senza un inghippo: il traffico crittografato non può essere monitorato nella DMZ, il che significa che gli addetti alla sicurezza IT sono costretti a far passare il traffico senza conoscerne il contenuto.

Mancanza di un controllo centralizzato

Poiché l'autenticazione, l'autorizzazione e il controllo possono essere applicati solo a ogni singolo host, il team di sicurezza centrale non può monitorare e applicare i criteri di sicurezza aziendali in modo efficace.

Considerato il valore dei vostri dati host critici, si tratta di falle significative nel sistema di sicurezza. La questione è: come potete proteggere i vostri dati senza modificare le applicazioni host che hanno impiegato decenni a svilupparsi? Come potete spostare i vostri host nel nuovo mondo della sicurezza?

Scongiurare nuove minacce alla sicurezza perpetuate da truffatori sempre più sofisticati è diventato uno stile di vita.

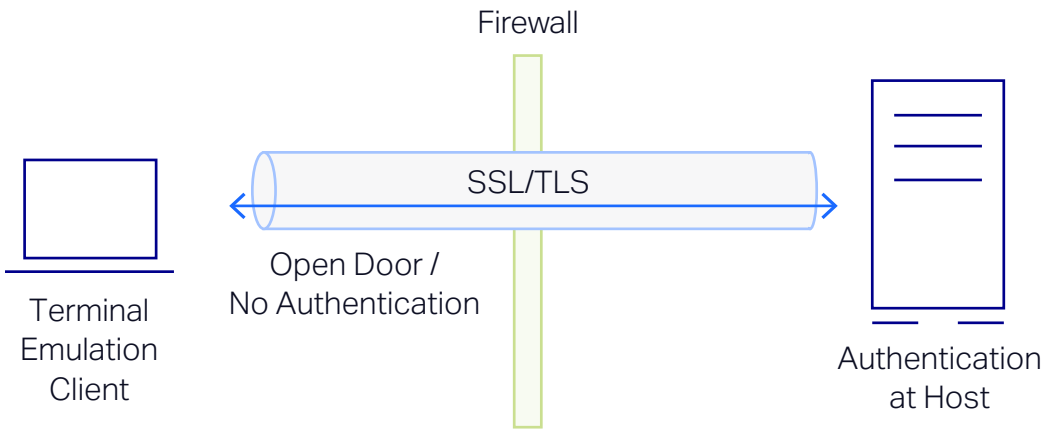

Figura 1. La sicurezza host di prima generazione offre una cifratura SSL/TLS diretta all'host, ma l'autenticazione non avviene fino a quando la connessione non ha raggiunto l'host.

Framework di sicurezza moderni

Scongiurare nuove minacce alla sicurezza perpetuate da truffatori sempre più sofisticati è diventato uno stile di vita. Purtroppo, non esiste un modo intrinsecamente sicuro per svolgere il proprio lavoro. La miglior difesa è l'applicazione di livelli di sicurezza, tra cui l'autenticazione avanzata e le tecnologie di autorizzazione, al fine di ridurre al minimo i rischi.

Ad esempio, le organizzazioni IT del governo degli Stati Uniti hanno stabilito delle infrastrutture a chiave pubblica (PKI) e hanno adottato l'utilizzo di smart card per supportare gli standard di identificazione personale, come il PIV (FIPS 201). Questi tipi di controlli vengono gradualmente adottati da organizzazioni commerciali alla ricerca della conformità con i nuovi standard, come PCI DSS, SOX e HIPAA.

I moderni sistemi IAM non sono stati progettati per funzionare con i sistemi host ereditati e viceversa. Ma se ci fosse un modo per integrare i due sistemi, estendendo la solida sicurezza gestita a livello centrale alle vostre applicazioni host, senza mettere a repentaglio le attività aziendali? Fortunatamente, un modo c'è e si chiama OpenText™ Host Access Management and Security Server (MSS).

L'aggiunta di livelli di sicurezza è una best practice che è possibile effettuare in fasi. Ma la realtà è che non si può avere una forte protezione senza una gestione forte. Questo è il motivo per cui le organizzazioni implementano sistemi IAM (Identity & Access Management). I sistemi IAM, come Active Directory, sono un componente chiave dei moderni framework di sicurezza. Consentono al reparto IT di concedere l'accesso, revocare l'accesso e controllare l'accesso ai dati, alle risorse e alle applicazioni aziendali da una posizione centrale.

Il problema è che i sistemi IAM non funzionano con i vostri host IBM, HP, UNIX e Unisys di lungo corso e ricchi di dati. Inoltre, non esiste un modo semplice per integrare i due sistemi. È difficile, rischioso e costoso riscrivere la logica dell'host eseguito nella vostra azienda, anche se in qualche modo riusciste a trovare un programmatore mainframe qualificato non ancora in pensione. È, inoltre, del tutto inaccettabile indebolire le vostre solide credenziali IAM per venire incontro alle deboli credenziali dell'accesso host. I costi in questione sono semplicemente troppo alti.

Fondamentalmente, si finirebbe con l'avere due distinte infrastrutture di sicurezza. Da un lato i vostri host, probabilmente gestiti da RACF o Top Secret. Dall'altro avreste tutto il resto, gestito da IAM. Incombenti su entrambe le infrastrutture sono le sempre più stringenti normative con le quali dovete confrontarvi.

Costruzione dell'alleanza host-IAM

I moderni sistemi IAM non sono stati progettati per funzionare con i sistemi host ereditati e viceversa. Ma se ci fosse un modo per integrare i due sistemi, estendendo la solida sicurezza gestita a livello centrale alle vostre applicazioni host, senza mettere a repentaglio le attività aziendali?

Fortunatamente, un modo c'è e si chiama OpenText™ Host Access Management and Security Server (MSS). MSS e i suoi componenti aggiuntivi collaborano con il vostro sistema IAM per gestire e proteggere a livello centrale l'accesso host tramite gli emulatori di terminale OpenText™ Reflection, OpenText™ Extra!, OpenText™ InfoConnect e OpenText™ Rumba+ . Si tratta di una soluzione non intrusiva che non richiede alcuna modifica alle vostre applicazioni host o al vostro sistema IAM.

Per ciascuna delle seguenti categorie di sicurezza, illustreremo come funzionano i moderni framework di sicurezza e spiegheremo come è possibile integrarli con i sistemi host utilizzando MSS:

Autenticazione centralizzata

Come funzionano i moderni framework di sicurezza: un sistema IAM applica rigidi criteri di autenticazione e sicurezza a tutta l'azienda.

Che cosa fa MSS: MSS include un server di amministrazione che sfrutta il sistema IAM per convalidare le credenziali di un utente prima di concedere l'accesso host. In altre parole, gli utenti non possono arrivare alla schermata di accesso host fino a quando non siano stati autenticati e autorizzati con solide credenziali IAM, purché siano chi dicono di essere. Ora, è possibile richiedere per l'accesso host la stessa solida autenticazione richiesta per accedere ad altri sistemi.

MSS facilita il processo di integrazione grazie al supporto di tutti i più comuni sistemi IAM, tra cui Active Directory, NetIQ eDirectory di OpenText™, IBM Tivoli Directory Server, OpenLDAP e Oracle Directory Server Enterprise Edition. MSS supporta anche una vasta gamma di tecnologie di autenticazione, fra cui Kerberos, NTLM, CRL OCSP, PKI e i certificati X.509 utilizzati con smart card come CAC e PIV.

Autorizzazione centralizzata

Come funzionano i moderni framework di sicurezza: un sistema IAM assicura che gli utenti abbiano accesso solo alle risorse e alle informazioni necessarie per svolgere il loro lavoro e niente di più.

Che cosa fa MSS: MSS rende possibile estendere gli schermi di autorizzazione IAM all'accesso host senza richiedere modifiche all'host o al flusso di lavoro degli utenti. Ad esempio, potete concedere o negare l'accesso in base al gruppo o al ruolo, consentendo a un utente di accedere al vostro mainframe 3270, ma non al vostro host Unisys. Potete aumentare ulteriormente il livello di autorizzazione con il proxy di sicurezza MSS. Il proxy di sicurezza fornisce un token brevettato a tempo limitato e firmato digitalmente, che utilizza la cifratura a chiave pubblica per impedire agli utenti non autorizzati di collegarsi all'host.

Con MSS, potete anche specificare cosa possono fare e non fare gli utenti. Ad esempio, potete rafforzare l'emulazione di terminale rimuovendo la capacità di un utente di modificare le macro o bloccare le impostazioni di connessione per TLS 1.2.

Dal server amministrativo MSS, è facile apportare al volo modifiche dopo l'installazione. All'avvio di una sessione successiva, gli utenti riceveranno le modifiche.

MSS facilita il processo di integrazione grazie al supporto di tutti i più comuni sistemi IAM, compresi:

- Active Directory
- NetIQ eDirectory
- IBM Tivoli Directory Server
- OpenLDAP
- Oracle Directory Server Enterprise Edition

Supporta anche una vasta gamma di tecnologie di autenticazione, tra cui:

- Kerberos
- NTLM
- CRL
- OCSP
- PKI,
- Certificati X.509 utilizzati con le smart card come CAC E PIV

Componenti di MSS

Un server amministrativo e un server di analisi sono inclusi con la licenza MSS. I seguenti prodotti aggiuntivi forniscono ulteriori funzionalità critiche:

Componente aggiuntivo MSS Security Proxy: per applicare il controllo degli accessi al perimetro tramite una tecnologia di sicurezza brevettata.

Componente aggiuntivo MSS Terminal ID Management: per allocare dinamicamente gli ID dei terminali in base a nome utente, nome DNS, indirizzo IP o pool di indirizzi.

Componente aggiuntivo MSS Automated Sign-On for Mainframe: per consentire agli utenti di immettere le proprie credenziali una sola volta e ottenere l'accesso autorizzato a tutti i sistemi aziendali, incluso il mainframe.

Componente aggiuntivo MSS PKI Automated Sign-On: per consentire l'accesso automatizzato PKI delle applicazioni ai vostri sistemi aziendali di importanza critica.

Con MSS e i suoi prodotti aggiuntivi, potete modernizzare la sicurezza host senza modificare le applicazioni host o il vostro sistema IAM.

Controllo centralizzato

Come funzionano i moderni framework di sicurezza: un sistema IAM documenta chi accede a quali risorse di rete e quando, fornendo agli amministratori di rete i dati di cui hanno bisogno per soddisfare i requisiti in materia di controllo.

Che cosa fa MSS: MSS utilizza il vostro attuale sistema IAM per autenticare gli utenti e autorizzare l'accesso host, registrando tutte le attività in una posizione centrale. Questo processo vi permette di sapere chi accede a quali host e quando. Assicura, inoltre, di avere una documentazione cartacea in caso di controlli.

Crittografia

Come funzionano i moderni framework di sicurezza: i dati vengono crittografati all'inizio della trasmissione, che sia all'interno o all'esterno del firewall, e vengono decrittografati alla ricezione. Questo processo protegge i dati e impedisce anche l'ispezione dei dati necessari nella DMZ.

Che cosa fa MSS: MSS funziona con il proxy di sicurezza MSS, che risiede tra il desktop e i vostri host. Il proxy di sicurezza accetta i pacchetti cifrati SSL/TLS e li decifra prima che siano consegnati all'host. Una volta decrittografati, i pacchetti possono essere monitorati tramite il rilevamento delle intrusioni, l'ispezione dei contenuti e altri dispositivi di sicurezza per possibili attacchi o perdite di dati.

Il proxy di sicurezza MSS non è come un semplice gateway o redirector SSL/TLS che accetta connessioni SSL/TLS senza prima autorizzare l'utente. Questi tipi di soluzioni permettono agli intrusi di accedere facilmente al vostro host. Con MSS, agli intrusi che tentano di effettuare una connessione SSL/TLS con l'host senza essere stati prima autenticati e autorizzati tramite il server amministrativo MSS, verrà negato l'accesso al proxy di sicurezza MSS. Il proxy di sicurezza utilizza un token sicuro brevettato da Micro Focus (ora parte di OpenText) per garantire che solo gli utenti autorizzati possano accedere alle risorse host.

MSS supporta livelli di cifratura fino a AES a 256 bit. Supporta anche i moduli di cifratura convalidati per FIPS 140-2, uno dei migliori standard di sicurezza del governo degli Stati Uniti. Questo alto livello di sicurezza consente di proteggere il vostro host da contenuti dannosi. Fornisce anche un framework di riferimento per l'aggiunta di livelli di sicurezza in base alle necessità.

Accesso a più host tramite una singola porta

Come funzionano i moderni framework di sicurezza: è possibile accedere a più server di backend tramite una singola porta di ascolto.

Che cosa fa MSS: MSS vi permette di utilizzare una singola apertura nel firewall (ad esempio, la porta 443) per accedere a tutti i vostri host. Successivamente, potrete aggiungere altri host senza cambiare nulla sul firewall. Oltre a ridurre il numero di porte necessarie per il monitoraggio, questa configurazione semplificata riduce anche la superficie di attacco della rete.

Controllo centralizzato delle configurazioni

Come funzionano i moderni framework di sicurezza: l'IT utilizza un sistema IAM per centralizzare la sicurezza, la gestione e la distribuzione di una vasta gamma di configurazioni di applicazioni in tutta l'azienda.

Che cosa fa MSS: MSS permette di gestire le operazioni di accesso all'host dalla vostra console MSS centrale. Potete concedere o negare l'accesso in base al gruppo o al ruolo, applicare rapidamente gli aggiornamenti di sicurezza e le modifiche di configurazione affinché siano allineati con le normative o le esigenze aziendali in evoluzione e apportare al volo le modifiche dopo l'installazione. In breve, potete configurare e bloccare centinaia o migliaia di desktop con facilità. E potete farlo con i vostri tempi, non quelli di altri.

Un vantaggio chiave di MSS è che sfrutta i vostri investimenti in sicurezza per autorizzare, autenticare e controllare l'accesso degli emulatori di terminali ai sistemi host da una posizione centrale. Di conseguenza, i problemi pratici e logistici associati all'applicazione di solide misure di sicurezza separatamente su ogni singolo host di backend vengono notevolmente ridotti.

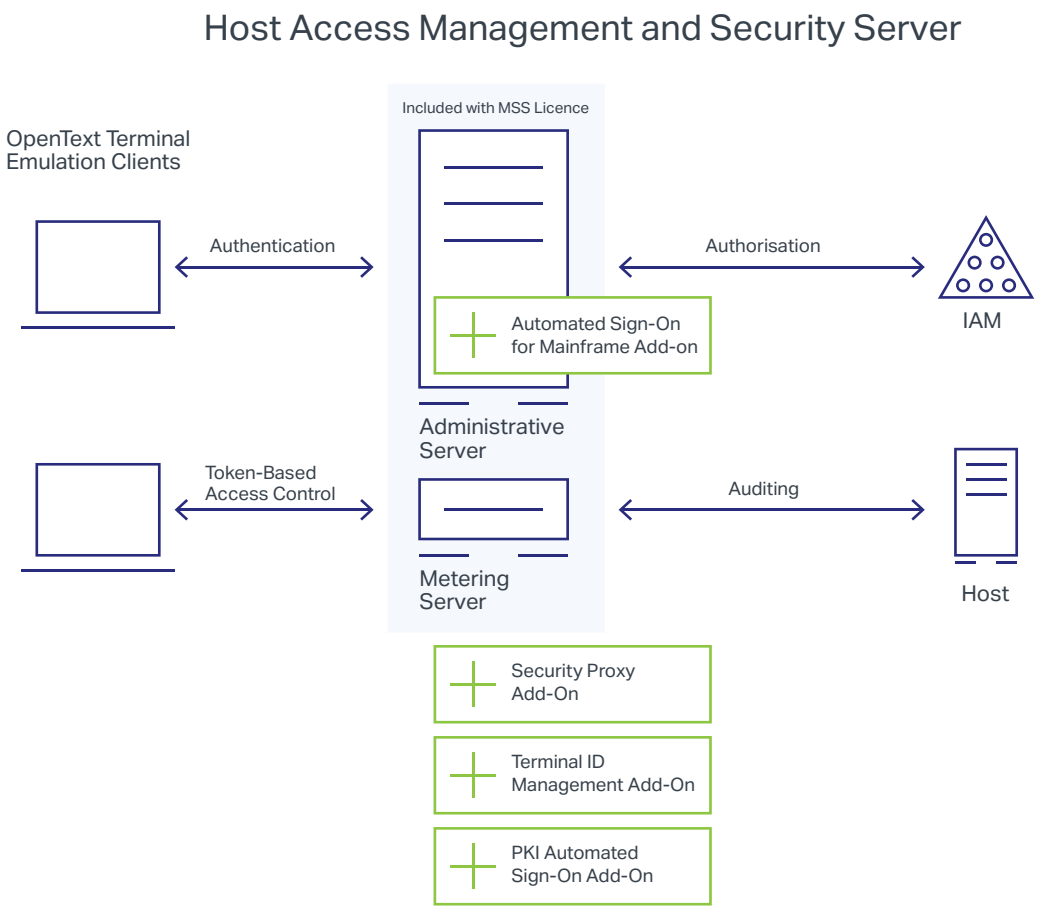

Figura 2. MSS posiziona un punto di controllo dell'accesso a monte dell'host in modo che l'utente debba autenticarsi ed essere autorizzato prima di accedere alle risorse dell'host.

Stessa protezione per tutto

Con MSS, potete finalmente offrire una moderna sicurezza multilivello alle vostre preziose risorse host, senza cambiare l'host o il vostro sistema IAM. Integrando questi due importanti sistemi aziendali attraverso MSS, potrete:

- Rafforzare la sicurezza delle vostre applicazioni e dati host critici.
- Snellire la gestione dell'accesso host.
- Massimizzare il vostro investimento nel sistema IAM estendendolo ai sistemi host.
- Facilitare la conformità con le odierne disposizioni di sicurezza di livello sempre più alto.
- Modernizzare in modo sicuro la sicurezza host senza interrompere i flussi di lavoro degli utenti o le attività aziendali.

Provate MSS voi stessi. Scaricate la guida alla valutazione dal sito **www.attachmate.com/products/mss/mss-eval-form.html** o contattate il vostro rappresentante commerciale.

Scoprite di più su
www.microfocus.com/opentext

Mettetevi in contatto con noi

Blog di Mark Barrenechea, CEO di OpenText

262-IT0064-001 | O | 05/23 | © 2023 Open Text

opentext™