Informe oficial

Integración de sistemas de host con marcos de seguridad modernos

El entorno que rodea sus sistemas de host ha cambiado. Hoy en día, estas "bestias de carga" de la empresa (enriquecidas con décadas de datos) no encajan en su marco de seguridad moderno. De hecho, su marco de seguridad moderno protege todo excepto sus hosts esenciales. Y, aún así, los requisitos normativos exigen una protección de datos equivalente para todo.

Este informe oficial muestra una forma práctica de integrar sus sistemas de host en el sistema de seguridad moderno para eliminar por fin la brecha tecnológica sin poner en peligro las operaciones de la empresa.

opentext™

Índice

página

El host se queda solo

Hace mucho, mucho tiempo, los sistemas de host vivían en un mundo seguro. Los datos viajaban entre el host y los terminales de confianza por una ruta protegida. El host sabía quién era el usuario, de dónde provenían los datos y a dónde iban.

Pero los tiempos han cambiado. Hoy en día, tenemos redes abiertas, arquitecturas orientadas a servicios y piratas informáticos cuyos ataques son más rápidos que los parches que puede proporcionar la TI. La seguridad del host no ha logrado seguir el ritmo. La seguridad tradicional de acceso al host deja los datos expuestos peligrosamente de varias maneras:

Autenticación débil y descentralizada

Una contraseña sencilla de ocho caracteres puede ser todo lo que se interponga entre un pirata informático malintencionado y sus datos de host esenciales. La autenticación basada en host por sí sola no puede aprovechar toda la potencia del sistema de gestión de identidades utilizado por el resto de la empresa.

Autorización débil y descentralizada

Cuando trabaja dentro de la red de la empresa, el usuario dispone de un fácil acceso a sus aplicaciones de host. Esto significa que un atacante solo tiene que robar las credenciales de host de ocho caracteres del usuario para penetrar en los campos de datos personales.

Auditoría descentralizada

La auditoría de acceso se realiza en cada host, en función del ID de host de cada usuario. Cuando hay varios hosts, los administradores de seguridad tienen que examinar los registros de cada uno (comparan el ID de usuario de cada host con el ID de usuario de la empresa) para realizar un seguimiento de auditoría completo.

Cifrado problemático

Hasta la llegada del cifrado SSL/TLS en los años 90, los datos y las contraseñas se transferían entre el cliente y el host en texto no cifrado. No había donde refugiarse de las miradas indiscretas. SSL/TLS solucionaron el problema del cifrado, pero el remedio no era perfecto: el tráfico cifrado no se puede controlar en la red perimetral (DMZ), lo que significa que la seguridad de TI está obligada a permitir el tráfico sin saber nada del contenido.

Falta de control centralizado

Dado que la autenticación, la autorización y la auditoría solo se pueden aplicar a hosts individuales, el equipo de seguridad central no puede controlar ni establecer de manera eficaz el uso de políticas de seguridad de la empresa.

Debido al valor de los datos de host esenciales, esto supone deficiencias de seguridad significativas. La pregunta es ¿cómo puede proteger sus datos sin cambiar las aplicaciones de host que han tardado décadas en desarrollarse? ¿Cómo puede trasladar sus hosts al nuevo mundo de la seguridad?

Detener las nuevas amenazas de seguridad perpetuadas por defraudadores cada vez más sofisticados se ha convertido en una forma de vida.

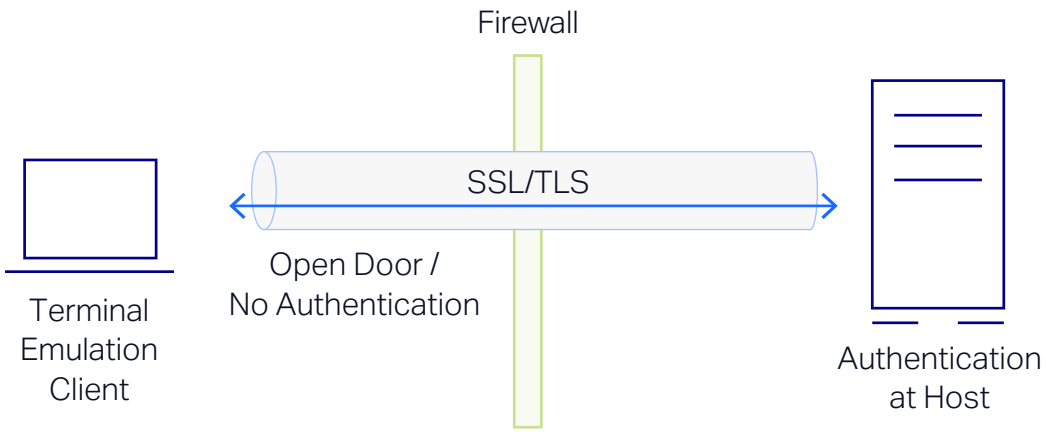

Figura 1. La seguridad de host de primera generación proporciona cifrado SSL/TLS aplicado al host directamente, pero la autenticación no se realiza hasta que la conexión haya alcanzado el host.

Los marcos de seguridad modernos

Detener las nuevas amenazas de seguridad perpetuadas por defraudadores cada vez más sofisticados se ha convertido en una forma de vida. Lamentablemente, no hay ningún método a prueba de errores para llevar esto a cabo. La mejor defensa es aplicar capas de seguridad, incluidas las tecnologías de autenticación y autorización avanzadas, para minimizar el riesgo.

Por ejemplo, las organizaciones de TI del gobierno de EE. UU. han establecido infraestructuras de clave pública (PKI) y han adoptado el uso de tarjetas inteligentes para respaldar los estándares de identificación personal como PIV (FIPS 201). Estos tipos de controles se van adoptando gradualmente por parte de entidades comerciales que quieren cumplir los nuevos estándares como PCI DSS, SOX e HIPAA.

Los modernos sistemas IAM no se diseñaron para trabajar con los antiguos sistemas de host, y viceversa. Pero ¿y si hubiera una forma de integrar los dos sistemas y ampliar la sólida seguridad centralizada a sus aplicaciones de host sin poner en peligro las operaciones empresariales? Afortunadamente, sí que la hay. Se llama OpenText™ Host Access Management and Security Server (MSS).

Añadir capas de seguridad es un enfoque basado en las mejores prácticas que puede llevar a cabo en fases. Pero la realidad es que no puede disponer de una seguridad sólida sin una gestión sólida. Es por esto por lo que las organizaciones implementan sistemas de gestión de acceso e identidades (IAM). Los sistemas IAM, como Active Directory, son un componente clave de los marcos de seguridad modernos. Permiten que la TI otorgue, revoque o audite el acceso a los datos, recursos y aplicaciones de la empresa desde una ubicación central.

El problema es que los sistemas IAM no funcionan con los antiguos hosts IBM, HP, UNIX y Unisys con gran cantidad de datos. No existe una manera sencilla de integrar los dos sistemas. Es caro, difícil y arriesgado reescribir la lógica del host que utiliza su empresa, aunque encuentre a un programador de mainframe cualificado que no esté jubilado. También es totalmente inaceptable debilitar sus sólidas credenciales de IAM para que estén al mismo nivel que las débiles credenciales de acceso del host. El precio es demasiado elevado.

En resumen, esto le deja con dos infraestructuras de seguridad independientes. Por un lado, tiene sus hosts, probablemente gestionados por RACF o Top Secret. Por otro lado, tiene todo lo demás, gestionado por IAM. Sobre estas infraestructuras acechan unas normativas cada vez más exigentes con las que tendrá que lidiar.

Formación de la alianza host-IAM

Los modernos sistemas IAM no se diseñaron para trabajar con los antiguos sistemas de host, y viceversa. Pero ¿y si hubiera una forma de integrar los dos sistemas y ampliar la sólida seguridad centralizada a sus aplicaciones de host sin poner en peligro las operaciones empresariales?

Afortunadamente, sí que la hay. Se llama OpenText™ Host Access Management and Security Server (MSS). MSS y sus componentes adicionales funcionan con su sistema IAM para gestionar y proteger de manera centralizada el acceso al host a través de los emuladores de terminal OpenText™ Reflection, OpenText™ Extra!, OpenText™ InfoConnect y OpenText™ Rumba+. Se trata de una solución no intrusiva que no requiere cambios en sus aplicaciones de host o su sistema IAM.

Para cada una de las siguientes categorías de seguridad, describiremos cómo funcionan los marcos de seguridad modernos y, a continuación, explicaremos cómo puede integrarlos en sus sistemas de host utilizando MSS:

Autenticación centralizada

Cómo funcionan los marcos de seguridad modernos: un sistema IAM aplica políticas de seguridad estrictas y autenticación sólida en toda la empresa.

Qué hace MSS: MSS incluye un servidor administrativo que aprovecha su sistema IAM para validar las credenciales de un usuario antes de conceder el acceso al host. En otras palabras, los usuarios no pueden llegar a la pantalla de conexión del host hasta que no se hayan autenticado y autorizado mediante credenciales sólidas de IAM, demostrando que son quienes dicen que son. Ahora puede solicitar la misma autenticación sólida para acceder al host que requiere para acceder a otros sistemas.

MSS facilita el proceso de integración mediante la compatibilidad con todos los sistemas IAM comunes, incluido Active Directory, NetIQ eDirectory by OpenText™, IBM Tivoli Directory Server, OpenLDAP y Oracle Directory Server Enterprise Edition. También es compatible con una variedad de tecnologías de autenticación, entre las que se incluye: Kerberos, NTLM, CRL, OCSP, PKI y certificados X.509 usados con tarjetas inteligentes como CAC y PIV.

Autorización centralizada

Cómo funcionan los marcos de seguridad modernos: un sistema IAM garantiza que los usuarios tengan acceso solo a la información y los recursos necesarios para realizar su trabajo, y nada más.

Qué hace MSS: MSS permite ampliar esquemas de autorización de IAM para acceder al host sin necesidad de realizar cambios en el host o el flujo de trabajo del usuario. Por ejemplo, puede otorgar o denegar el acceso en función del grupo o función; es decir, puede permitir que un usuario acceda a su mainframe 3270, pero no a su host Unisys. Puede llevar la autorización a un nivel superior con el proxy de seguridad de MSS. El proxy de seguridad proporciona un testigo patentado con firma digital de tiempo limitado que utiliza el cifrado de clave pública para impedir que usuarios no autorizados se conecten al host.

Con MSS, también puede especificar lo que pueden hacer los usuarios. Por ejemplo, puede fortalecer la emulación de terminal; para ello, debe eliminar la capacidad del usuario para editar macros o debe bloquear los ajustes de conexión para TLS 1.2.

Desde el servidor administrativo de MSS, es fácil realizar ajustes sobre la marcha posteriores a la instalación. Los usuarios verán los cambios la próxima vez que inicien sesión.

MSS facilita el proceso de integración gracias a la compatibilidad con todos los sistemas IAM comunes, incluidos:

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

También es compatible con una variedad de tecnologías de autenticación, entre las que se incluyen:

- Kerberos
- NTLM
- CRL
- OCSP
- PKI
- Los certificados X.509 que se utilizan con tarjetas inteligentes como CAC y PIV

Componentes de MSS

Se incluye un servidor administrativo y un servidor de medición en su licencia de MSS. Los siguientes productos adicionales proporcionan funciones esenciales adicionales:

MSS Security Proxy Add-On: aplica el control de acceso en los perímetros con una tecnología de seguridad patentada.

MSS Terminal ID Management Add-On: asigna ID de terminal de forma dinámica en función del nombre de usuario, el nombre DNS, la dirección IP o el repositorio de direcciones.

MSS Automated Sign-On for Mainframe Add-On: permite que los usuarios introduzcan sus credenciales solo una vez para obtener acceso autorizado a todos los sistemas de la empresa, incluido el mainframe.

MSS PKI Automated Sign-On Add-On: permite que las aplicaciones automatizadas PKI puedan entrar en los sistemas fundamentales de la empresa.

Con MSS y sus productos adicionales, puede modernizar la seguridad de host sin cambiar sus aplicaciones de host o su sistema IAM.

Auditoría centralizada

Cómo funcionan los marcos de seguridad modernos: un sistema IAM documenta quién ha accedido a determinados recursos de la red y cuándo; además, proporciona a los administradores de red los datos que necesitan para cumplir con los requisitos de las auditorías.

Qué hace MSS: MSS utiliza su sistema IAM existente para autenticar a los usuarios y autorizar el acceso al host, y registra toda la actividad en una ubicación central. Este proceso le garantiza que sabrá quién ha accedido a un determinado host y cuándo. También garantiza que dispondrá de un registro por escrito cuando se realice la auditoría.

Cifrado

Cómo funcionan los marcos de seguridad modernos: los datos se cifran al inicio de la transmisión, ya sea dentro o fuera del firewall, y se descifran en el momento de la recepción. Además de proteger los datos, este proceso también evita la inspección de datos necesaria en la DMZ.

Qué hace MSS: MSS trabaja con el proxy de seguridad de MSS, que se ubica entre los equipos de escritorio y los hosts. El proxy de seguridad acepta paquetes cifrados SSL/TLS y los descifra antes de que se envíen al host. Una vez descifrados, los paquetes se pueden supervisar mediante detección de intrusos, inspección de contenido y otros dispositivos de seguridad para detectar posibles ataques o fugas de datos.

El proxy de seguridad de MSS no es una simple puerta de enlace SSL/TLS o un redirector que acepta conexiones SSL/TLS sin autorizar primero al usuario. Estos tipos de soluciones proporcionan a los intrusos un viaje gratis hasta el host. Con MSS, a los intrusos que intentan establecer una conexión SSL/TLS con el host, sin superar la autenticación ni recibir autorización mediante el servidor administrativo de MSS, se les denegará el acceso en el proxy de seguridad de MSS. El proxy de seguridad utiliza un testigo seguro patentado de Micro Focus (ahora parte de OpenText) para garantizar que solo los usuarios autorizados acceden a los recursos del host.

MSS es compatible con intensidades de cifrado AES de hasta 256 bits. También es compatible con módulos de cifrado validados para FIPS 140-2, uno de los estándares de seguridad más exigentes del gobierno de los EE. UU. Este alto nivel de seguridad significa que puede proteger su host frente a contenido malicioso. También proporciona un marco para añadir capas de seguridad según sea necesario.

Acceso a varios hosts a través de un solo puerto

Cómo funcionan los marcos de seguridad modernos: se puede acceder a varios servidores secundarios a través de un puerto de escucha.

Qué hace MSS: MSS le permite utilizar una única apertura en el firewall (por ejemplo, puerto 443) para acceder a todos los hosts. Posteriormente, puede añadir otros hosts sin cambiar nada en el firewall. Además de reducir el número de puertos que debe supervisar, esta configuración simplificada también reduce la superficie de la red susceptible de ataque.

Control de configuración centralizado

Cómo funcionan los marcos de seguridad modernos: la TI utiliza un sistema IAM para proteger, gestionar e implantar de forma centralizada una amplia variedad de configuraciones de aplicaciones en toda la empresa.

Qué hace MSS: MSS le permite gestionar las operaciones de acceso al host desde la consola central de MSS. Puede otorgar o denegar el acceso en función del grupo o función, aplicar rápidamente las actualizaciones de seguridad y los cambios de configuración para adecuarse a las necesidades empresariales y normativas en constante cambio, y realizar ajustes posteriores a la instalación sobre la marcha. En resumen, puede configurar y bloquear cientos o miles de equipos de escritorio con facilidad. Y puede hacerlo según su programación, no la de otra persona.

Una ventaja clave de MSS es que aprovecha su inversión en seguridad actual para autorizar, autenticar y auditar el acceso de emulación de terminal a sistemas de host desde una ubicación central. Como resultado, los problemas prácticos y logísticos asociados a la aplicación de potentes medidas de seguridad en cada host secundario se reducen considerablemente.

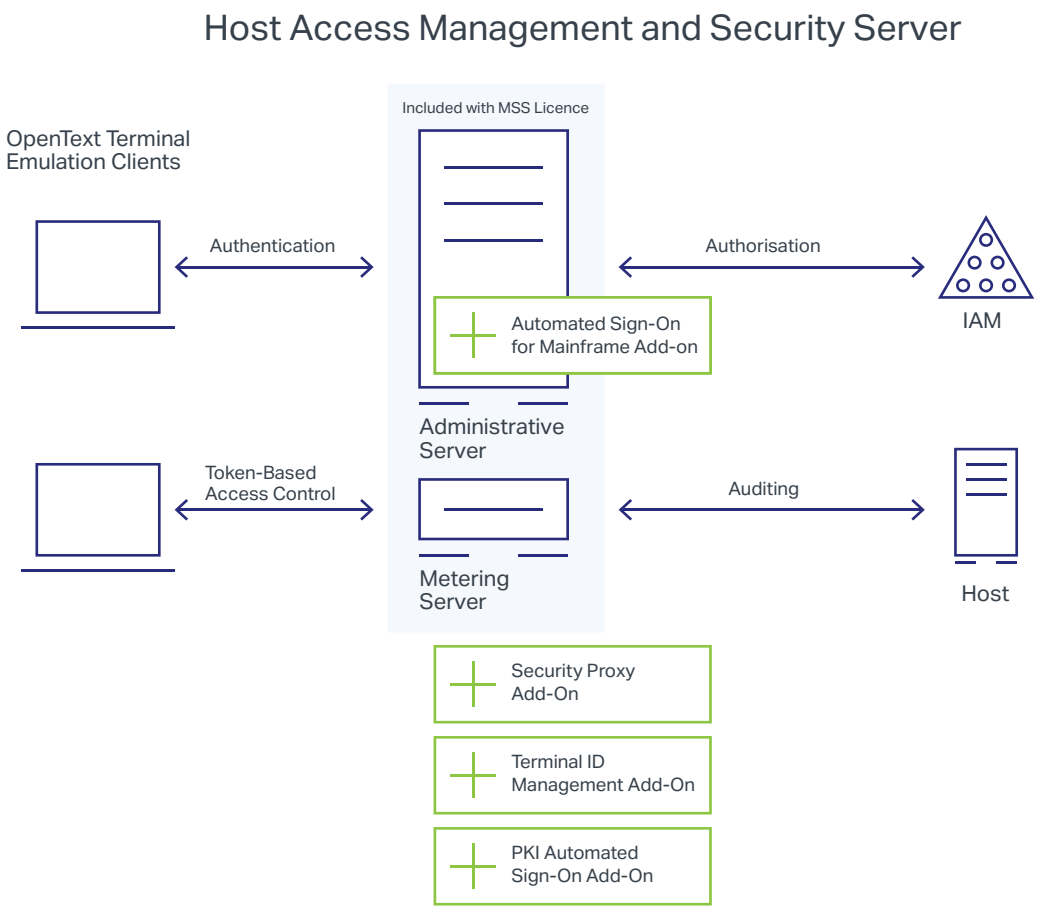

Figura 2. MSS funciona como un punto de control de acceso antes del host, lo que garantiza que los usuarios se hayan autenticado y autorizado para acceder a los recursos del host.

Protección equivalente para todo

Con MSS, puede ofrecer seguridad moderna y de varias capas a sus valiosos activos de host sin cambiar el host o su sistema IAM. Mediante la integración de estos dos sistemas fundamentales de la empresa a través de MSS, puede:

- Reforzar la seguridad de sus datos y aplicaciones de host esenciales.
- Simplificar la gestión de acceso al host.
- Maximizar su inversión en IAM al ampliar sus ventajas a los sistemas de host.
- Facilitar el cumplimiento de las normativas de seguridad más elevadas de hoy en día.
- Modernizar de manera segura la seguridad de host sin interrumpir los flujos de trabajo de usuario u operaciones comerciales.

Pruebe MSS. Descargue la guía de evaluación en **www.attachmate.com/products/mss/mss-eval-form.html** o póngase en contacto con su representante de ventas.

Más información en
www.microfocus.com/opentext

Póngase en contacto con nosotros

El blog de Mark Barrenechea, director general de OpenText

262-ES0064-001 | O | 05/23 |

opentext™