White paper

Integrar sistemas de host com metodologias modernas de segurança

O mundo mudou em torno dos seus sistemas de host. Hoje em dia, essas peças corporativas indispensáveis, recheadas com décadas de dados, não são mais compatíveis com sua metodologia moderna de segurança. Na verdade, sua metodologia moderna de segurança protege tudo, menos seus hosts essenciais. Ainda assim, as exigências regulamentares demandam que a proteção de dados seja igual para tudo.

Este white paper revela uma forma prática de levar os sistemas de host para o patamar de segurança moderna, finalmente eliminando essa lacuna na segurança, sem prejudicar as operações de negócios.

opentext™

Sumário

página

O host autônomo

Era uma vez, um mundo seguro em que viviam os hosts. Os dados do host percorriam um caminho protegido, indo e voltando de um terminal confiável. O host sabia quem era o usuário, de onde vinham e para onde se dirigiam os dados.

Os tempos mudaram. Atualmente, temos redes abertas, arquiteturas voltadas para os serviços e hackers que hackeiam mais rápido do que o departamento de TI consegue impedir. A segurança do host não conseguiu acompanhar. A segurança de acesso de host tradicional deixa os dados perigosamente expostos de várias maneiras:

Autenticação fraca e descentralizada
Senhas simples de oito caracteres podem ser o único obstáculo entre os hackers mal intencionados e os seus dados de host essenciais. A autenticação baseada em host, por si só, não pode aproveitar ao máximo o potencial do sistema de gerenciamento de identidades usado no restante da empresa.

Autorização fraca e descentralizada
Depois de fazer o login na rede corporativa, o usuário tem acesso fácil aos seus aplicativos de host. Isso significa que um invasor precisa apenas roubar as credenciais de oito caracteres de um usuário do host para invadir os campos de dados pessoais.

Auditoria descentralizada
Cada host executa a auditoria de acesso de host com base na ID de host do usuário. Quando há vários hosts envolvidos, os administradores de segurança precisam examinar os registros em todos eles (comparando o ID de usuário em cada host ao ID de usuário da empresa) para criar uma trilha de auditoria completa.

Criptografia problemática
Até a chegada da criptografia SSL/TLS na década de 1990, os dados e as senhas trafegavam entre o cliente e o host em texto sem criptografia. Não havia proteção contra os olhares curiosos. A SSL/TLS resolveu o problema da criptografia, mas não sem um porém: o tráfego criptografado não pode ser monitorado no DMZ, o que significa que a segurança de TI é forçada a permitir o tráfego sem ter nenhuma informação sobre o conteúdo.

Falta de controle centralizado
Devido ao fato de que a autenticação, a autorização e a auditoria podem ser aplicadas apenas em hosts individuais, a equipe de segurança central não pode monitorar de forma eficaz e assegurar o uso das políticas de segurança da empresa.

Dado o valor dos seus dados do host essenciais, isso significa falhas de segurança consideráveis. A pergunta é: como você pode proteger seus dados sem alterar os aplicativos de host que levaram décadas para serem desenvolvidos? Como é possível mover os hosts para o novo mundo da segurança?

Evitar novas ameaças à segurança mantidas pelos impostores cada vez mais sofisticados se tornou um modo de vida.

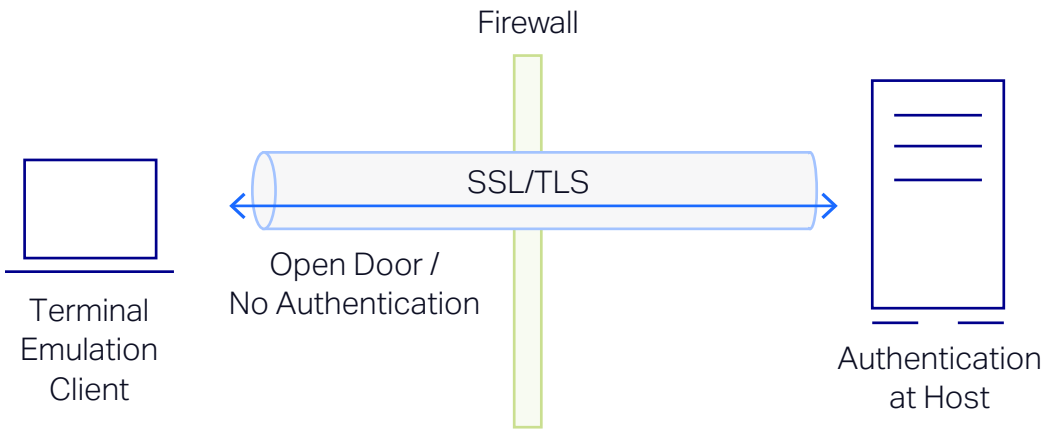

Figura 1. A primeira geração de segurança de host fornece criptografia SSL/TLS diretamente para o host, mas a autenticação não ocorre até que a conexão chegue ao host.

Metodologias modernas de segurança

Evitar novas ameaças à segurança mantidas pelos impostores cada vez mais sofisticados se tornou um modo de vida. Infelizmente, não existe um jeito 100% garantido de fazer isso. A melhor defesa é aplicar camadas de segurança, incluindo tecnologias avançadas de autenticação e autorização para minimizar os riscos.

Por exemplo, as organizações de TI dos EUA estabeleceram as infraestruturas de chave pública (PKIs) e adotaram o uso de smart cards para compatibilidade com os padrões de identificação pessoal, como o PIV (FIPS 201). Esses tipos de controle estão sendo adotados gradualmente pelas entidades comerciais à medida em que elas buscam ficar em conformidade com os novos padrões, como PCI DSS, SOX e HIPPA.

Os sistemas de IAM modernos nunca foram projetados para funcionar com sistemas de host legados e vice-versa. Mas o que acontece se houver uma maneira de integrar os dois sistemas, ampliando a segurança forte e gerenciada centralmente para os seus aplicativos host sem comprometer as operações de negócios? Felizmente, existe uma maneira. Ela se chama OpenText™ Host Access Management and Security Server (MSS).

Adicionar níveis de segurança é a melhor abordagem que pode ser aplicada em fases. Mas a realidade é que você não pode ter segurança forte sem gerenciamento forte. É por isso que as organizações implementam sistemas de Gerenciamento de identidade e acesso (IAM). Sistemas IAM, como o Active Directory, são componentes importantes das metodologias modernas de segurança. Eles permitem que a TI conceda ou revogue o acesso e faça a auditoria do acesso aos dados, recursos e aplicativos corporativos a partir de um local central.

O problema é que os sistemas IAM não funcionam com os hosts IBM, HP, UNIX e Unisys antigos e ricos em dados. E não há uma forma simples de integrar os dois sistemas. É difícil, arriscado e caro reconfigurar a lógica de hosts que controla a empresa, mesmo que você encontre um programador de mainframe capacitado que ainda não se aposentou. Também é inaceitável enfraquecer suas credenciais fortes de IAM para corresponder às credenciais fracas de login no host. Os custos envolvidos são altos demais.

Basicamente, isso deixa você com duas infraestruturas de segurança. De um lado, você tem seus hosts, provavelmente gerenciados por RACF ou Top Secret. Do outro, você tem tudo o mais sendo gerenciado por IAM. Depender de duas grandes infraestruturas está cada vez mais difícil devido às exigências regulatórias com as quais você deve lidar.

Criação da aliança host-IAM

Os sistemas de IAM modernos nunca foram projetados para funcionar com sistemas de host legados e vice-versa. Mas o que acontece se houver uma maneira de integrar os dois sistemas, ampliando a segurança forte e gerenciada centralmente para os seus aplicativos host sem comprometer as operações de negócios?

Felizmente, existe uma maneira. Ela se chama OpenText™ Host Access Management and Security Server (MSS). O MSS e seus componentes complementares funcionam com seu sistema IAM para gerenciar e proteger o acesso ao host de maneira centralizada por meio de seus emuladores de terminal OpenText™ Reflection, OpenText™ Extra!, OpenText™ InfoConnect, e OpenText™ Rumba+. Essa é uma solução não invasiva que não necessita de alterações em seus aplicativos de host ou no sistema IAM.

Para cada uma das seguintes categorias de segurança, destacaremos como as metodologias modernas de segurança funcionam e, em seguida, explicaremos como você pode integrá-las aos seus sistemas de host usando o MSS:

Autenticação centralizada

Como as metodologias modernas de segurança funcionam: um sistema IAM assegura o uso obrigatório de autenticação forte e de rígidas políticas de segurança em toda a empresa.

O que o MSS faz: o MSS inclui um servidor administrativo que aproveita o seu sistema IAM para validar as credenciais de um usuário antes de conceder o acesso ao host. Em outras palavras, os usuários não poderão ir para a tela de login do host até terem sido autenticados e autorizados com as fortes credenciais do IAM, comprovando que são quem afirmam ser. Agora você pode exigir a mesma autenticação forte para o acesso ao host que é usada para o acesso aos outros sistemas.

O MSS facilita o processo de integração dando suporte a todos os sistemas IAM comuns, incluindo Active Directory, NetIQ eDirectory pelo OpenText™, IBM Tivoli Directory Server, OpenLDAP, e Oracle Directory Server Enterprise Edition. Ele também oferece suporte a uma variedade de tecnologias de autenticação, incluindo Kerberos, NTLM, CRL, OCSP, PKI e certificados X.509 usados com smart cards como CAC e PIV.

Autorização centralizada

Como as metodologias modernas de segurança funcionam: um sistema IAM garante que os usuários tenham acesso somente aos recursos e informações necessários para realizar suas tarefas e nada além disso.

O que o MSS faz: o MSS possibilita ampliar os esquemas de autorização IAM para o acesso ao host sem a necessidade de alterar o fluxo de trabalho do host ou do usuário. Por exemplo, você pode conceder ou negar o acesso com base em grupo ou função, permitindo que um usuário acesse seu mainframe 3270, mas não seu host Unisys. Você pode reforçar a autorização com o proxy de segurança do MSS. A segurança de proxy fornece um token patenteado com limitação de tempo e com assinatura digital que usa criptografia de chave pública para evitar que usuários não autorizados se conectem ao host.

Com o MSS, você também pode especificar o que os usuários podem fazer ou não. Por exemplo, você pode proteger emulação de terminal, impedindo que um usuário edite macros ou bloqueando as configurações de conexão do TLS 1.2.

A partir do servidor administrativo MSS, é fácil fazer ajustes pós-instalação simultaneamente. Na próxima vez em que os usuários iniciarem uma sessão, eles receberão as alterações.

O MSS facilita o processo de integração pelo suporte a todos os sistemas IAM comuns, incluindo:

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

Ele também oferece suporte a uma variedade de tecnologias de autenticação, incluindo:

- Kerberos
- NTLM
- CRL
- OCSP
- PKI
- Certificados X.509 usados com smart cards como CAC e PIV

Componentes do MSS

Um servidor administrativo e um servidor métrico estão incluídos na sua licença do MSS. Os produtos complementares a seguir fornecem funções essenciais e adicionais:

Complemento de proxy de segurança do MSS: assegura o uso obrigatório do controle de acesso no perímetro com tecnologia de segurança patenteada.

Complemento de gerenciamento de ID de terminal do MSS: aloca dinamicamente as IDs de terminal com base no nome de usuário, nome DNS, endereço IP ou pool de endereços.

Login automatizado de MSS para complemento de Mainframe: permite que os usuários insiram suas credenciais apenas uma vez para obter acesso autorizado a todos os sistemas da empresa, incluindo o mainframe.

Complemento de login automatizado de PKI do MSS: permite, pelo PKI, o login automatizado do aplicativo em seus principais sistemas empresariais.

Com o MSS e seus produtos complementares, você pode modernizar a segurança de host sem alterar seus aplicativos de host ou o sistema IAM.

Auditoria centralizada

Como as metodologias modernas de segurança funcionam: um sistema IAM documenta quando e quem acessou os recursos de rede, munindo os administradores de rede com os dados de que precisam para cumprir os requisitos de auditoria.

O que o MSS faz: o MSS usa o seu sistema IAM para autenticar os usuários e autorizar o acesso ao host, registrando todas as atividades em um local central. Esse processo garante que você saiba quem acessou qual host e quando isso ocorreu. Isso também garante que você tenha registros impressos quando houver auditorias.

Criptografia

Como as metodologias modernas de segurança funcionam: os dados são criptografados no início da transmissão, dentro ou fora do firewall e são descriptografados ao serem recebidos. Ao passo que esse processo protege os dados, ele também impede inspeção de dados necessária no DMZ.

O que o MSS faz: o MSS funciona com o proxy de segurança do MSS, que fica entre seus desktops e seus hosts. O proxy de segurança aceita os pacotes criptografados SSL/TLS e os descriptografa antes que eles sejam entregues ao host. Depois de descriptografados, os pacotes podem ser monitorados pela detecção de intrusão, inspeção de conteúdo e outros dispositivos de segurança para prevenir possíveis ataques ou vazamento de dados.

O proxy de segurança do MSS não é como um gateway ou redirecionador SSL/TLS que aceita as conexões SSL/TLS sem antes autorizar o usuário. Esses tipos de soluções abrem totalmente o caminho do host para os invasores. Com o MSS, os invasores que tentarem fazer uma conexão SSL/TLS com o host, sem antes serem autenticados e autorizados pelo servidor administrativo do MSS, terão o acesso negado no proxy de segurança do MSS. O proxy de segurança usa um token de segurança patenteado da Micro Focus (agora parte da OpenText) para garantir que somente usuários autorizados cheguem aos recursos do host.

O MSS suporta o fortalecimento de criptografia até AES de 256 bits. Ele também suporta módulos criptográficos validados para FIPS 140-2, um dos mais elevados padrões de segurança do governo dos EUA. Esse alto nível de segurança significa que você pode proteger o seu host de conteúdo malicioso. Ele também fornece uma metodologia para adicionar camadas de segurança conforme o necessário.

Acesso a vários hosts por meio de uma única porta

Como as metodologias modernas de segurança funcionam: vários servidores back-end podem ser acessados por uma única porta de escuta.

O que o MSS faz: o MSS permite usar uma única abertura no firewall (por exemplo, porta 443) para acessar todos os seus hosts. Posteriormente, você pode adicionar outros hosts sem alterar nada no firewall. Além de reduzir o número de portas que você precisa monitorar, essa configuração simplificada também reduz a superfície de ataque da sua rede.

Controle de configuração centralizado

Como as metodologias modernas de segurança funcionam: a TI usa um sistema IAM centralmente para proteger, gerenciar e implantar uma vasta gama de configurações de aplicativo em toda empresa.

O que o MSS faz: o MSS permite que você gerencie as operações de acesso ao host a partir do console de MSS central. Você pode conceder ou negar acesso com base em grupo ou função, aplicar rapidamente as atualizações de segurança e as alterações de configuração para se adequar às alterações regulatórias ou às suas necessidades comerciais e fazer ajustes pós-instalação simultaneamente. Em resumo, você pode configurar e bloquear centenas ou milhares de desktops com facilidade. E pode você pode fazer isso na sua programação e não na de outra pessoa.

Uma das principais vantagens do MSS é que ele aproveita os investimentos existentes para autorizar, autenticar e fazer a auditoria do acesso de emulação de terminal em sistemas de host a partir de um local central. Como resultado, os problemas práticos e logísticos relacionados à aplicação de medidas de segurança em cada host em back-end são significativamente reduzidos.

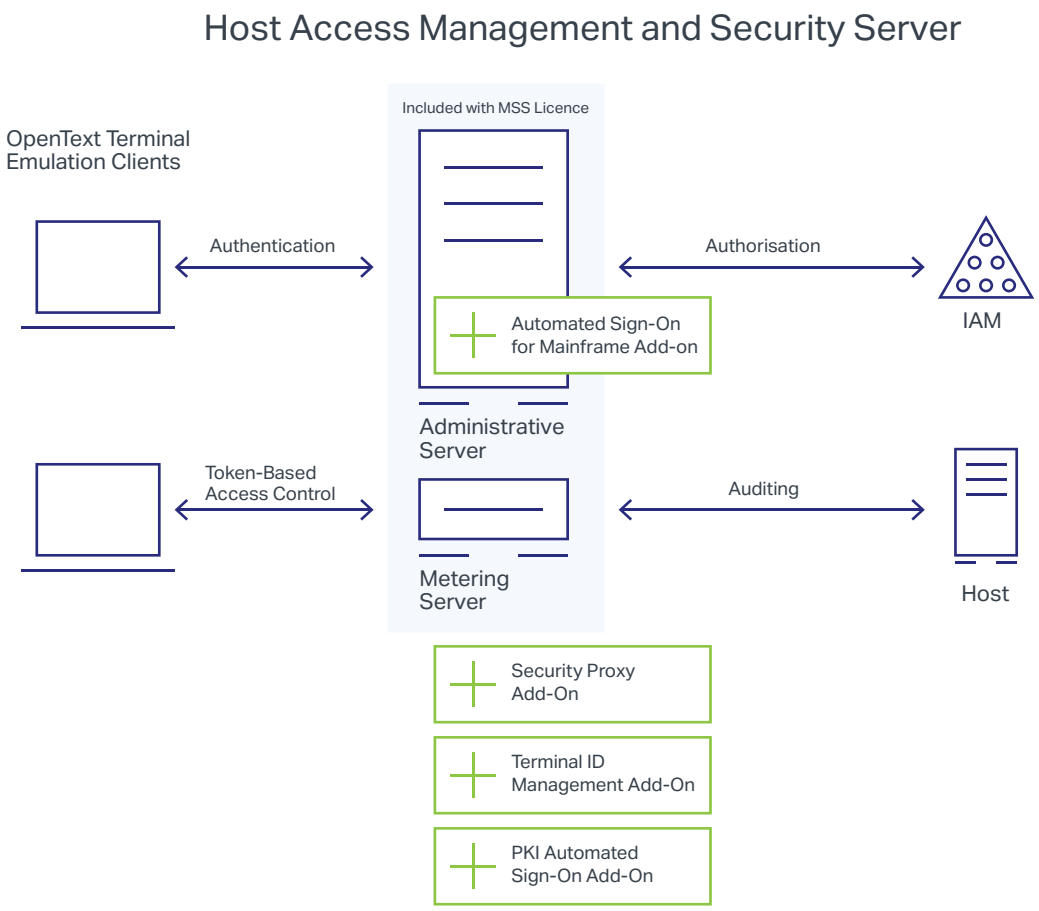

Figura 2. O MSS funciona como um ponto de controle de acesso na frente do host, o que garante que os usuários sejam autenticados e autorizados antes de obterem acesso aos recursos do host.

Proteção equivalente para tudo

Com o MSS, você pode finalmente fornecer segurança moderna multicamada para os seus valiosos ativos de host sem alterar o host ou o sistema IAM. Ao integrar esses dois sistemas corporativos essenciais pelo MSS, você pode:

- Reforçar a segurança dos seus aplicativos e dados de host essenciais.
- Agilizar o gerenciamento de acesso ao host.
- Maximizar o seu investimento em IAM ao estender o IAM para os sistemas de host.
- Facilitar a conformidade com os níveis mais altos de segurança exigidos hoje em dia.
- Modernizar a segurança do host sem interromper os fluxos de trabalho dos usuários ou as operações da empresa.

Teste você mesmo o MSS. Faça o download do guia de avaliação em **www.attachmate.com/products/mss/mss-eval-form.html** ou entre em contato com o seu representante de vendas.

Saiba mais em
www.microfocus.com/opentext

Conecte-se conosco

Blog de Mark Barrenechea, CEO da OpenText

262-PB0064-001 | O | 06/23 |

opentext™