RESUMO DA SOLUÇÃO

Como posso proteger as credenciais com privilégios em datacenters tradicionais e virtuais, nuvens privadas e públicas e ambientes híbridos?

ca technologies

O gerenciamento e a proteção de credenciais com privilégios são essenciais para reduzir os riscos e atender aos requisitos de conformidade. As organizações precisam avaliar as soluções de gerenciamento de senhas com privilégios em termos de profundidade dos controles, escopo da cobertura e nível de alinhamento de nuvem que elas fornecem. O CA Privileged Access Manager atende a essas três dimensões oferecendo uma solução de última geração para gerenciamento de credenciais com privilégios que promove a redução dos riscos de TI, melhora a eficiência operacional e protege o investimento da organização, oferecendo suporte a infraestruturas tradicionais, virtualizadas e de nuvem híbrida.

Resumo executivo

Desafio

A adoção da virtualização e da computação na nuvem está aumentando a importância e a complexidade de um problema antigo: gerenciar e proteger de maneira eficaz as senhas de contas com privilégios. O gerenciamento de senhas com privilégios em infraestruturas tradicionais (equipamentos de rede, servidores, mainframes, etc.) é um problema de segurança e conformidade de longa data. A grande quantidade de credenciais com privilégios codificadas nos aplicativos complica ainda mais a situação. Exemplos desses tipos de credencial são pares de chaves SSH e chaves codificadas em PEM usadas para acessar recursos da Amazon Web Services (AWS).

Oportunidade

Uma proteção eficaz das credenciais com privilégios em toda a empresa híbrida pode ajudar a organização a reduzir os riscos de exploração de invasores externos e pessoal interno mal-intencionado. As organizações têm a oportunidade de adotar abordagens de gerenciamento de acesso com privilégios que oferecem os 12 recursos essenciais, explicados neste resumo, para reduzir os riscos de auditorias malsucedidas e violações de conformidade, perda de dados de alto valor e interrupção onerosa do serviço, que são problemas resultantes de contas com privilégios desprotegidas.

Benefícios

O CA Privileged Access Manager fornece um conjunto abrangente de controles para proteger e gerenciar qualquer tipo de credencial para todos os tipos de recurso, onde quer que estejam localizados e de uma forma que acompanhe o ritmo dos ambientes de nuvem híbrida da atualidade, permitindo que as organizações obtenham uma redução maior de riscos, custos de propriedade e carga de trabalho operacional do que seria possível com abordagens alternativas que não fornecem uma profundidade equivalente de controles, amplitude de cobertura e alinhamento com a computação na nuvem.

Seção 1:

Noções básicas do gerenciamento de senhas com privilégios

As senhas de usuários com privilégios (a partir deste ponto, chamadas apenas de senhas com privilégios) distinguem-se das senhas de usuários comuns pois protegem de maneira uniforme o acesso aos recursos mais confidenciais da organização, ou seja, as contas administrativas (por exemplo, admin, root, SYS e sa) e os recursos associados, usados para configurar e controlar a infraestrutura de TI de uma organização. Devido ao risco envolvido, é bastante óbvio que gerenciar e proteger tais credenciais é importante. Essa questão é confirmada pelos inúmeros conjuntos de requisitos associados que são codificados em padrões e regulamentos de segurança aplicados com frequência, como NIST Special Publication 800-53 e Payment Card Industry Data Security Standard (PCI DSS).

Sem contar com os requisitos regulatórios, o gerenciamento de senhas com privilégios é uma prática recomendada de uma perspectiva de gerenciamento de risco, mas também é essencial para enfrentar a variedade de práticas inseguras que são comuns nas organizações da atualidade. Senhas fracas, obsoletas ou expostas (por exemplo, porque foram mantidas em um lembrete ou uma planilha), o uso de muitas senhas, o compartilhamento de senhas, a falta de uma atribuição clara de contas compartilhadas e a ausência de opções para autenticação forte e revogação centralizada são apenas alguns dos problemas que costumamos encontrar.

De acordo com o Verizon Data Breach Investigations Report de 2015, 95% das violações são o resultado de credenciais roubadas, enquanto outros 10% foram resultantes do uso indevido das credenciais por pessoal interno confiável.[1]

O problema real, porém, é o potencial de que qualquer uma dessas condições resulte em um spear phishing bem-sucedido, ataques direcionados e, por fim, roubo de dados, sem mencionar as violações de conformidade. Precisa de provas? De acordo com o Verizon Data Breach Investigations Report de 2015, 95% das violações são o resultado de credenciais roubadas, enquanto outros 10% foram resultantes do uso indevido das credenciais por pessoal interno confiável.[1] Descobertas como essas deixam bem claro por que as organizações da atualidade precisam utilizar uma solução corporativa, como o CA Privileged Access Manager, para gerenciamento, proteção e controle de acesso de credenciais com privilégios.

O impacto da nuvem híbrida

Os problemas tradicionais mencionados acima são apenas a ponta do iceberg. A adoção generalizada da nuvem híbrida é inevitável por conta das vantagens de custo atrativo, adaptabilidade e capacidade de resposta das configurações que ela oferece, em que os serviços e aplicativos de TI utilizam uma infraestrutura tradicional e virtualizada que abrange datacenters corporativos e na nuvem. Além de todos os benefícios, no entanto, as nuvens híbridas geram outros desafios para o gerenciamento de senhas com privilégios, incluindo:

- Maior volume/escala — as demandas operacionais e a facilidade de implantação de máquinas virtuais resultam no aumento do número de entidades que exigem acesso com privilégios (e, portanto, senhas com privilégios)
- Escopo maior — o poder concentrado dos consoles de gerenciamento de virtualização e nuvem adiciona outro tipo de recurso/conta com privilégios
- Maior dinamismo — novos servidores/sistemas podem ser adicionados sob demanda, sem mencionar a opção em massa (por exemplo, 10, 20 ou mais por vez)
- Potencial para a criação de ilhas de identidades — cada serviço de nuvem diferente tem seus próprios armazenamentos e infraestruturas de identidades[2]

Além dos desafios apresentados pela nuvem híbrida, os gerentes de segurança de TI precisam manter em mente dois outros aspectos do problema de gerenciamento de senhas com privilégios ao avaliarem as possíveis soluções. Primeiro, eles precisam levar em consideração o cenário de máquina para máquina ou aplicativo para aplicativo (A2A), em que as senhas usadas por um sistema ou aplicativo para obter acesso a outro sistema ou aplicativo são codificadas no aplicativo de acesso ou disponibilizadas para ele em um arquivo de configuração com texto sem formatação. O segundo item a considerar é a questão muitas vezes negligenciada de que a maioria das organizações também pode ter milhares de chaves (por exemplo, para implementações de SSH) que, embora não sejam senhas tradicionais e orientadas para frases, ainda funcionam como credenciais de autenticação para contas com privilégios e, portanto, exigem gerenciamento e proteção para reduzir os riscos associados.

O resultado final é que, na era da nuvem híbrida, o gerenciamento de senhas com privilégios se tornou mais importante e complexo do que nunca.

Seção 2:

Solução de gerenciamento de acesso com privilégios da CA Technologies

O CA Privileged Access Manager é uma solução abrangente para o gerenciamento de acesso com privilégios. Como tal, além de controlar o acesso, monitorar e gravar as atividades de usuários com privilégios em ambientes de nuvem híbrida, o CA Privileged Access Manager incorpora os recursos que são necessários em uma solução de última geração para gerenciamento de senhas com privilégios. É importante que as equipes de segurança de TI reconheçam que, embora o gerenciamento e a proteção de senhas sejam ações valiosas, também atuam como um meio para atingir objetivos maiores. Em particular, elas são o passo inicial (ou complementar) no processo mais amplo e igualmente importante de fazer um controle e gerenciamento real do acesso a recursos de alto risco. Se a distinção parecer sutil, isso ocorre em grande parte porque, na prática, as implementações funcionais de mecanismos de autenticação (ou seja, senhas) e o controle de acesso raramente são aplicados separadamente, portanto, geralmente são lembrados em conjunto.

Em qualquer caso, os objetivos do projeto para os recursos de gerenciamento de senhas com privilégios incluídos no CA Privileged Access Manager são iguais àqueles aplicados no restante da solução. Nosso objetivo específico é oferecer uma solução que não apenas forneça um conjunto abrangente de controles e recursos para uma ampla gama de metas e casos de uso, mas que também faça isso de maneira consistente com arquiteturas, práticas e opções de entrega da era da nuvem.

Controles abrangentes

Quando se trata de avaliar as soluções de gerenciamento de senhas com privilégios, recomendamos observar primeiro se a solução incorpora um conjunto abrangente de controles para ajudar a equipe de segurança a enfrentar os riscos decorrentes das abordagens tradicionais de criação, gerenciamento e uso de credenciais administrativas confidenciais. Áreas específicas que devem ser verificadas incluem detecção, armazenamento, imposição de diretivas, recuperação e capacidade de oferecer suporte a uma evolução ininterrupta para uma implementação completa de gerenciamento de acesso com privilégios.

Seção 3:

12 recursos essenciais do gerenciamento de acesso com privilégios

Nº 1. Detecção automatizada/facilitada

Quando não houver um meio para garantir a detecção automatizada ou facilitada, o processo de iniciar o gerenciamento de senhas com privilégios poderá ser oneroso, sem mencionar a grande quantidade de erros ou omissões que deixam o ambiente de computação da organização vulnerável aos sofisticados ataques da atualidade. Por esse motivo, o CA Privileged Access Manager inclui uma variedade de métodos para detectar dispositivos, sistemas, aplicativos, serviços e contas, incluindo a utilização de associações de portas conhecidas, informações de diretório, consoles de gerenciamento e APIs (Application Programming Interfaces - Interfaces de Programação de Aplicativos). Ele usa, por exemplo, as APIs disponíveis para soluções de gerenciamento de virtualização e nuvem com suporte para alertar os administradores quando outras máquinas virtuais forem criadas. Além disso, a solução facilita a importação em massa de listas de sistema a partir de arquivos de texto, bem como a criação de entradas ad hoc pelo console de gerenciamento. Por fim, também é importante compreender que optamos por evitar técnicas de detecção mais disruptivas (e possivelmente mais arriscadas) que exigem agentes com base no destino para criar um vínculo ou gancho na pilha TCP local.

Nº 2. Armazenamento seguro

Um armazenamento criptografado fornece um ponto de controle centralizado e é a chave para eliminar métodos de armazenamento inseguros (como planilhas) que facilitam o compartilhamento e o comprometimento das credenciais. O armazenamento do CA Privileged Access Manager é uma solução compatível com FIPS 140-2 Nível 1 e segura para as credenciais. Ele utiliza a criptografia AES de 256 bits para armazenar com segurança todos os tipos de credencial, não apenas senhas. Recursos adicionais interessantes da solução incluem:

- A opção de utilizar os HSM (Hardware Security Modules - Módulos de Segurança de Hardware) integrados, como aqueles da SafeNet e Thales, para fazer uma implementação de FIPS 140-2 Nível 2 ou Nível 3. Ela é particularmente importante para clientes e casos de uso de grande visibilidade e avessos a riscos, como aqueles envolvidos com sistemas financeiros e bancários, nos quais é recomendável armazenar as chaves usadas para criptografar credenciais separadamente das credenciais criptografadas. Várias opções de implantação do CA Privileged Access Manager têm suporte, incluindo os equipamentos de hardware com placas PCI integradas, os equipamentos virtuais que fazem chamadas para equipamentos de HSM conectados à rede e os equipamentos de qualquer tipo que fazem chamadas para uma oferta de "HSM como serviço" da AWS.
- Rotinas criptográficas de caixa branca comprovadas que protegem as chaves de criptografia durante o uso (ou seja, na memória) em um sistema. Essa abordagem foi projetada para impedir que hackers captem/juntem partes das chaves monitorando a memória e as APIs criptográficas padrão e contornando alternativas inferiores, com base em agrupamento de chaves ou simples ofuscação. A inclusão desta tecnologia é particularmente importante para os casos de uso A2A, nos quais o sistema de acesso também deve armazenar as credenciais e há uma possibilidade maior de que o sistema seja comprometido (por exemplo, porque se encontra em um local relativamente exposto).

Nº 3. Imposição automatizada de diretivas

O CA Privileged Access Manager automatiza a criação, o uso e a mudança de senhas, eliminando a tendência de reutilizar senhas ou confiar em senhas fracas (e fáceis de lembrar). Com o CA Privileged Access Manager, diretivas flexíveis podem ser configuradas para aumentar a complexidade da senha, implementar requisitos de mudança, como troca periódica de senhas (por exemplo, diariamente ou semanalmente) ou em resposta a um evento específico (por exemplo, após cada uso) e controlar o uso (por exemplo, permitindo o acesso apenas em períodos específicos ou exigindo autorizações duplas/múltiplas para o acesso com senha). Como essas diretivas podem ser aplicadas de forma hierárquica e aos grupos de recursos de destino, diferentes requisitos e recursos podem ser atendidos em diversos destinos e a imposição também se torna efetivamente dinâmica, já que qualquer recurso adicionado a um grupo herda automaticamente as diretivas daquele grupo. Nos bastidores, o CA Privileged Access Manager também interage diretamente com os recursos de destino afetados para garantir que todas as credenciais permaneçam sincronizadas (ou seja, quando elas forem alteradas em uma extremidade, também serão alteradas na outra).

Nº 4. Recuperação e apresentação/uso seguros

Colocar credenciais com privilégios em um armazenamento é inútil se elas não puderem ser recuperadas e usadas de forma segura. O primeiro passo desse processo é a autenticação precisa de quem, ou o que, no caso de aplicativos e scripts, está tentando acessar/usar uma credencial. Nesse caso, o CA Privileged Access Manager aproveita por completo a infraestrutura de identidades existente, com integração ao Active Directory e a diretórios compatíveis com LDAP, bem como sistemas de autenticação, como o Radius. Também há suporte para:

- Tokens de dois fatores (por exemplo, por meio do CA Advanced Authentication ou outras soluções, como aquelas da RSA e SafeNet)
- Certificados X.509/PKI
- PIV/CAC necessários para garantir a conformidade de setor federal com os decretos HSPD-12 e OMB-11-11
- SAML
- Técnicas multifatoriais compostas (por exemplo, combinar senhas com tokens da RSA)

No modo preferencial de operações, o CA Privileged Access Manager posteriormente apresenta a credencial solicitada ao sistema de destino, em nome da entidade que solicita o acesso (por exemplo, usuário ou aplicativo). Essa abordagem oferece vários benefícios adicionais de segurança. Em primeiro lugar, ao contrário do que acontece nas soluções simples de check-in/check-out, as credenciais nunca são vistas pelas entidades que solicitam acesso nem distribuídas para elas. Essa medida reduz muito o potencial de exposição. Além disso, como a autenticação no sistema de destino é totalmente automatizada e os usuários nunca precisam gerenciar nem lembrar das senhas, diretivas podem ser implementadas para aumentar drasticamente a complexidade da senha. Como todo o acesso aos destinos ocorre por meio do CA Privileged Access Manager, a solução também pode fornecer atribuição completa de atividades de usuários com privilégios, até mesmo para contas de administrador compartilhadas.

Por uma questão de integridade, também é importante mencionar que todas as comunicações de rede entre as entidades que solicitam acesso, o CA Privileged Access Manager e os destinos administrados são criptografadas por SSL. Além disso, o CA Privileged Access Manager oferece suporte a um modo alternativo de operação, no qual as entidades que solicitam acesso podem recuperar diretamente e enviar as credenciais necessárias para sistemas de destino por conta própria.

Nº 5. Transição ininterrupta para gerenciamento completo de acesso com privilégios

O CA Privileged Access Manager oferece às organizações originalmente focadas apenas no gerenciamento de senhas todos os recursos necessários para fazer a transição para uma implementação completa do gerenciamento de acesso com

privilégios quando elas percebem que há necessidade. Alguns dos recursos mais notáveis à disposição do departamento de segurança de TI quando ele estiver pronto para aproveitá-los incluem:

- Controle de acesso granular com base em funções e fluxos de trabalho associados (por exemplo, solicitar/autorizar permissões adicionais)
- Estabelecimento automatizado de conexão/sessão com recursos de destino (com suporte para RDP, SSH, web e vários outros modos/opções de acesso)
- Monitoramento em tempo real de sessões de usuários com privilégios, além de imposição com base em diretivas de atividades permitidas/negadas (por exemplo, que comandos podem ser empregados por um usuário específico)
- Registro em log, incluindo integração com SIEM com base em syslog
- Gravação completa de sessões com reprodução como DVR para ir diretamente a eventos de interesse
- Leapfrog Prevention que impede que os usuários burlem as permissões e aproveitem destinos acessíveis para obter acesso a outros destinos não autorizados

Além disso, a implementação desses recursos adicionais não poderia ser mais fácil. O CA Privileged Access Manager fornece todas as funcionalidades de gerenciamento de senhas com privilégios e controle de acesso como uma única solução, totalmente integrada. Ele também fornece gerenciamento unificado de diretivas em toda a solução, uma abordagem que simplifica ainda mais a implementação e a administração.

Cobertura abrangente

A segunda área de alto nível que deve ser avaliada ao escolher uma solução para gerenciamento de senhas com privilégios é o escopo da cobertura que ela proporciona. Em outras palavras, para o conjunto abrangente de controles identificados acima, a que tipos de entidades de acesso, credenciais e sistemas de destino a solução realmente oferece suporte?

Nº 6. Cobertura abrangente para destinos tradicionais

O CA Privileged Access Manager inclui uma grande variedade de conectores de sistema de destino, proporcionando a integração imediata a todos os tipos de infraestruturas de TI, dispositivos de rede, sistemas e aplicativos, incluindo:

- Contas de domínio, administrador local e serviço do Windows®
- Distribuições populares de Linux® e UNIX®
- AS/400
- Dispositivos de rede da Cisco e Juniper
- Sistemas com base em Telnet/SSH
- SAP
- Remedy
- Bancos de dados ODBC/JDBC
- Servidores de aplicativos e sistemas

Como uma solução extensível, o CA Privileged Access Manager também fornece recursos flexíveis de personalização para que as organizações possam estender o suporte mais facilmente para sistemas proprietários e desenvolvidos internamente.

Nº 7. Suporte para virtualização e consoles de gerenciamento de nuvem

A cobertura do CA Privileged Access Manager para gerenciar e proteger as credenciais não se limita a destinos tradicionais. Ela se estende a soluções populares de virtualização e nuvem, incluindo VMware vSphere, VMware NSX, Amazon Web Services e Microsoft® Online Services. Além disso, os recursos que se aplicam a essas soluções não se limitam a cada instância de máquinas virtuais, aplicativos ou serviços associados. A cobertura se estende também aos consoles de gerenciamento correspondentes, que, devido ao poder que exercem, devem ser reconhecidos como recursos com privilégios.

Nº 8. Suporte para autenticação de máquina para máquina

Como mencionado anteriormente, os seres humanos não são os únicos usuários de credenciais com privilégios. Na maioria das organizações, inúmeros aplicativos e sistemas também estão habilitados a acessar recursos confidenciais, como outros aplicativos ou bancos de dados. Isso normalmente é feito por meio da incorporação de credenciais associadas ao código do aplicativo que solicita acesso ou da disponibilização dele em um arquivo de configuração em tempo de execução. Nenhuma dessas opções é particularmente segura ou gerenciável. O CA Privileged Access Manager oferece cobertura para esses casos de uso A2A e permite que os desenvolvedores incluam um cliente leve do CA Privileged Access Manager em seus aplicativos. Essa abordagem oferece aos "aplicativos com privilégios" todos os recursos de que eles precisam para fazer o registro com o CA Privileged Access Manager, recuperar dinamicamente as senhas necessárias e, em seguida, protegê-las enquanto estiverem na memória do sistema local. Além disso, vários mecanismos estão disponíveis para autenticar os aplicativos com privilégios e verificar a integridade deles antes que o CA Privileged Access Manager libere as credenciais solicitadas.

Ao usar o CA Privileged Access Manager para cenários A2A, as organizações podem eliminar com mais eficácia as credenciais A2A expostas/inseguras armazenando-as centralmente, automatizar o gerenciamento de credenciais e a imposição de diretivas A2A e simplificar as atividades de auditoria e conformidade relacionadas.

Nº 9. Suporte para gerenciamento de chaves

Além de oferecer suporte às operações criptográficas, muitos tipos de chave também servem como tokens para confirmar a identidade. Embora essas chaves não sejam senhas no sentido tradicional, elas ainda funcionam como senhas e estão sujeitas a ameaças, riscos e desafios semelhantes, como cópia, compartilhamento, exposição não intencional e backdoors não auditadas. Como essas chaves geralmente são incorporadas ou usadas de maneira transparente em soluções para proteger os usuários contra a complexidade relativa que possuem, elas também são mais propensas a se tornarem órfãs e/ou serem proliferadas ao longo do tempo. Faz sentido, portanto, aplicar nessas credenciais alternativas muitos dos controles usados para gerenciar e proteger senhas. De fato, as práticas recomendadas para enfrentar as ameaças relacionadas incluem:

- Mover as chaves autorizadas para locais protegidos
- Trocar todas as chaves regularmente (para garantir o eventual encerramento do acesso em caso de chaves vazadas)
- Impor restrições de fonte para chaves autorizadas[3]
- Impor restrições de comando para chaves autorizadas

Desse modo, o CA Privileged Access Manager tem controles e outros recursos para lidar com tipos de credenciais alternativas, incluindo chaves SSH e chaves codificadas em PEM usadas para acessar consoles de gerenciamento e recursos da AWS. Em outras palavras, com o CA Privileged Access Manager, essas credenciais podem ser: (1) armazenadas, (2) trocadas e controladas por diretivas configuradas e (3) recuperadas e usadas de forma a minimizar o potencial de roubo ou exposição.

Entrega na era da nuvem

Na era da nuvem híbrida, outro fator principal para o sucesso de uma solução de gerenciamento de senhas com privilégios é sua adequação não apenas física, mas também em termos de alinhamento com as necessidades e os recursos de rede na nuvem.

Nº 10. Opções de entrega no local, na máquina virtual e na nuvem

O CA Privileged Access Manager oferece suporte a três opções convenientes de implantação que ajudam as organizações a acompanharem o ritmo das arquiteturas complexas da nuvem híbrida:

- Um equipamento físico protegido — disponível em vários modelos para montagem em rack tradicional no datacenter corporativo
- Uma Amazon Machine Instance (AMI) — pré-configurada para implantação com a infraestrutura do Amazon EC2
- Um equipamento virtual compatível com OVF — pronto e pré-configurado para implantação em ambientes VMware

Independentemente das opções de implantação usadas, as organizações obtêm uma solução que permite o gerenciamento de toda a infraestrutura da nuvem híbrida.

Nº 11. Arquitetura e abordagem alinhadas à nuvem

O CA Privileged Access Manager foi criado com o propósito de incorporar inúmeros recursos que o tornam um "bom cidadão" em ambientes de nuvem híbrida. Aqui estão três exemplos:

- Proteção e detecção automática — Em ambientes de nuvem híbrida, os operadores podem criar (ou desativar) um número qualquer de sistemas com um único comando. O CA Privileged Access Manager lida com essa situação utilizando APIs aplicáveis para detectar automaticamente os recursos virtualizados e de nuvem e, em seguida, provisionar (ou desprovisionar) as diretivas adequadas de gerenciamento de acesso e credenciais.
- Tentativa de evitar ilhas de identidades (ou seja, federação de identidades) — Como uma forma de eliminar ilhas separadas de informações de identidade, o CA Privileged Access Manager aproveita totalmente qualquer tipo de infraestrutura de identidades que a organização já tiver. Outra maneira, específica para implementações da AWS, é oferecer suporte a usuários efêmeros. Essa é uma abordagem que evita que as organizações precisem manter as informações de identidade separadas no subsistema de gerenciamento de identidades e acesso da AWS.
- Permissão de automação — Uma API abrangente permite acesso programático e automação de todas as funcionalidades do CA Privileged Access Manager (por exemplo, por meio de sistemas externos de gerenciamento e orquestração).

Nº 12. Confiabilidade e escalabilidade prontas para a nuvem

O gerenciamento de credenciais com privilégios é um elemento essencial da infraestrutura de TI de uma organização. Essa afirmação é ainda mais verdadeira quando a implementação é estendida para oferecer suporte a casos de uso A2A, que operam de forma totalmente automatizada. Para isso, o CA Privileged Access Manager inclui funcionalidades nativas de agrupamento e distribuição de carga, capazes de atender aos requisitos de alta disponibilidade e escalabilidade dos maiores e mais exigentes ambientes. Em comparação com alternativas comuns, com o CA Privileged Access Manager não há necessidade de investir em balanceadores de carga separados e externos, não há atrasos de desempenho, típicos em abordagens ativas/passivas, e não é preciso ter licenças adicionais de recursos "opcionais". Se desejado e operacionalmente aceitável do ponto de vista da latência, os agrupamentos do CA Privileged Access Manager ainda podem ser configurados para permitir redundância entre ambientes de nuvem e datacenters afastados geograficamente.

O CA Privileged Access Manager oferece uma solução de última geração para gerenciamento de credenciais com privilégios, desenvolvida para promover a redução dos riscos de segurança e melhorar a eficiência operacional na infraestrutura da empresa híbrida.

Seção 4:

Conclusão: Conquistando o gerenciamento de credenciais com privilégios na era da nuvem

O gerenciamento e a proteção de credenciais com privilégios são essenciais para reduzir os riscos e garantir a conformidade com os requisitos relacionados. A complexidade e a importância desse problema também estão cada vez maiores, já que os ambientes de nuvem híbrida apresentam consoles de gerenciamento com potência sem precedentes e capacidade de adicionar/remover literalmente centenas de sistemas de destino com apenas alguns cliques do mouse.

As organizações que desejarem analisar essa área extremamente importante da estratégia de segurança das informações precisam avaliar as soluções dos candidatos em termos de profundidade dos controles, escopo da cobertura e nível de alinhamento de nuvem que eles fornecem. Conforme mencionado acima, o CA Privileged Access Manager atende a essas três dimensões para oferecer exatamente o que as organizações da atualidade precisam: uma solução de última geração para gerenciamento de credenciais com privilégios, desenvolvida para promover a redução dos riscos de TI, melhorar a eficiência operacional e proteger o investimento de cada uma delas, oferecendo suporte a infraestruturas tradicionais, virtualizadas e de nuvem híbrida.

ca technologies

Conecte-se à CA Technologies em ca.com/br

A CA Technologies (NASDAQ: CA) cria software que acelera a transformação das empresas e permite que elas aproveitem as oportunidades da economia dos aplicativos. O software está no cerne de todas as empresas, em todos os setores. Do planejamento ao desenvolvimento e do gerenciamento à segurança, a CA está trabalhando com empresas de todo o mundo para mudar a maneira como vivemos, fazemos negócios e nos comunicamos – usando dispositivos móveis, as nuvens privada e pública e os ambientes distribuídos e de mainframe. Obtenha mais informações em ca.com/br.

1 Verizon Data Breach Investigations Report, 2015.

2 *"New Platforms, New Requirements. Privileged Identity Management for the Hybrid Cloud"*, documentação técnica da CA, março de 2013.

3 *"Managing SSH Keys for Automated Access - Current Recommended Practice"*, IETF Draft, abril de 2013.

 CS200-169152_1215