RELATÓRIO TÉCNICO

Soluções da Centrify para PCI DSS

Conteúdo

O Centrify Server Suite® (CSS) permite a consolidação e gerenciamento centralizado de identidades de usuários e servidores, autenticação de usuário, controle de acesso baseado em função e registro de sessão. O Centrify Privilege Service™ (CPS) oferece gerenciamento de senha de conta compartilhada e acesso remoto seguro a recursos. Juntos, eles ajudam a tratar de muitos dos requisitos de PCI DSS relacionados a gerenciamento e uso privilegiado de conta e controle sobre o acesso a recursos que estão no escopo de PCI DSS.

Resumo

O Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) possui e mantém o Padrão de Segurança de Dados (DSS), um rigoroso conjunto de requisitos que todos os mercadores, processadores de pagamento, fornecedores de ponto de vendas e instituições financeiras devem seguir. As pesadas sanções definidas pelos membros do PCI são determinadas para garantir que todos os mercadores e fornecedores de serviço trabalhem para manter a confiança do consumidor nos cartões de pagamento, uma vez que a perda de confiança poderia causar impacto negativo na receita.

O PCI DSS 3.1 é composto por 12 requisitos disseminados em seis domínios. Como a preocupação central do PCI é a proteção dos dados do titular do cartão, esses requisitos enfocam o acesso de usuário aos servidores que hospedam esses dados ou pelos quais tais dados passam.

Esse relatório técnico examina cada um dos 12 requisitos e identifica habilidades do Server Suite e do Privilege Service que os consumidores podem aproveitar como auxílio para obter conformidade.

Requisitos de PCI Resumo de Aplicabilidade

Server Suite (Standard Edition, Enterprise Edition e Platinum Edition) e Privilege Service contribuem com sua postura de conformidade de PCI DSS em uma gama de diferentes áreas. Eles oferecem controles de segurança para gerenciar e restringir acesso privilegiado de usuário a sistemas e dados de PCI DSS. Eles também podem ajudar a reduzir o escopo de PCI ao isolar recursos de PCI, controlar acesso de usuário, comunicação de servidor para servidor (isto é, a comunicação desses servidores com servidores não confiáveis) e a criptografia de dados entre eles.

A tabela abaixo oferece uma visão de alto nível dos domínios/requisitos para os quais as soluções da Centrify contribuem com conformidade de PCI DSS.

Domínio de PCI	Requisito	Server Suite e Privilege Service
Criar e manter uma rede segura	1. Instale e mantenha uma configuração de firewall para proteger os dados de titulares de cartão	SIM
	2. Não utilize os padrões do fornecedor para senhas do sistema e outros parâmetros de segurança	SIM
Proteger os dados de titulares de cartão	3. Proteja os dados de titulares de cartão armazenados	SIM
	4. Criptografe a transmissão de dados de titulares de cartão em redes abertas e públicas	SIM
Manter um Programa de gestão de vulnerabilidade	5. Use e atualize regularmente softwares ou programas de antivírus	N/A
	6. Desenvolva e mantenha sistemas e aplicativos seguros	SIM
Implementar medidas sólidas de controle de acesso	7. Restrinja o acesso aos dados de titulares de cartão com o princípio da necessidade de conhecer	SIM
	8. Atribua um ID único a cada pessoa com acesso a um computador	SIM
	9. Restrinja o acesso físico aos dados dos titulares de cartões	N/A
Monitorar e testar as redes regularmente	10. Acompanhe e monitore todo o acesso aos recursos da rede e aos dados de titulares de cartão	SIM
	11. Teste regularmente os sistemas e processos de segurança	SIM
Manter uma Política de segurança de informações	12. Mantenha uma política que trate da segurança das informações para todo o pessoal	SIM

Requisitos de PCI

Requisito 1: Instale e mantenha uma configuração de firewall para proteger os dados de titulares de cartão

Nº	Requisito	Server Suite e Privilege Service
1.2	Criar uma configuração de firewall que restringe conexões entre redes não confiáveis e qualquer componente de sistema no ambiente de dados do titular do cartão	**O Server Suite** oferece aplicação com base em política de grupo de um firewall com base em iptables. Ao usar esta política, os administradores podem restringir o tráfego de entrada a portas específicas de endereços de IP específicos. **O Server Suite Platinum Edition** oferece proteções adicionais para o servidor ao exigir autenticação antes de qualquer comunicação. Esse requisito pode ser aplicado tanto a comunicações de entrada como de saída para garantir que os sistemas de PCI só podem se comunicar com outros sistemas de PCI. Uma vez que o **Privilege Service** oferece suporte à conectividade remota sem VPN, é possível estabelecer, de forma seletiva, uma sessão remota com um recurso distinto identificado por seu hostname ou endereço de IP
1.3	Proibir acesso público direto entre a Internet e qualquer componente de sistema no ambiente de dados do titular do cartão.	Quando autenticação mútua é necessária, o **Server Suite Platinum Edition** evitará a comunicação com sistemas não confiáveis ou qualquer sistema fora da rede, já que eles não podem autenticar e não são confiáveis. **O Server Suite Platinum Edition** reforça a forma mais segura de proteção de firewall de rede, garantindo que um computador permitirá comunicação apenas com outros sistemas confiáveis

Requisito 2: Não utilize os padrões do fornecedor para senhas do sistema e outros parâmetros de segurança

Nº	Requisito	Server Suite e Privilege Service
2.1	Sempre mudar os padrões do fornecedor e remover ou desabilitar contas padrão antes de instalar um sistema na rede	**O Privilege Service** armazena senhas de conta privilegiadas compartilhadas em um armazenamento seguro. Uma vez que essas senhas são subordinadas ao gerenciamento do **Privilege Service**, o **Privilege Service** fará ciclos com as senhas a partir de seu padrão.
2.3	Criptografar todos os acessos administrativos de não console usando criptografia forte. Usar tecnologias como SSH, VPN ou TLS para gerenciamento com base em web e outro acesso administrativo de não console	Por estar em uso em muitos sistemas, o telnet não é seguro e deve ser substituído com SSH, que possibilita segurança de transporte de rede. Versões mais recentes do OpenSSH oferecem suporte para Kerberos para autenticação do usuário e, quando combinados com o **Server Suite,** eliminam a necessidade de gerenciar as chaves estáticas SSH. A Centrify também oferece uma versão compilada e fácil de instalar do último OpenSSH, o que permite que os consumidores tenham certeza de que eles têm uma versão consistente em todos os sistemas para o maior nível de segurança.

Requisito 2 (continuação): Não utilize os padrões do fornecedor para senhas do sistema e outros parâmetros de segurança

Nº	Requisito	Server Suite e Privilege Service
2.3 cont.	Criptografar todos os acessos administrativos de não console usando criptografia forte. Usartecnologias como SSH, VPN ou TLS para gerenciamento com base em web e outro acesso administrativo de não console	Com o **Privilege Service**, todas as sessões de conta compartilhada privilegiadas para recursos são criptografadas. Desde o navegador do usuário ao Cloud Connector no local via HTTPS e, então, via SSH ou RDP até o endpoint. Além disso, o **Privilege Service** oferece suporte a autenticação de dois fatores para usuários que fazem login no portal de **Privilege Service** portal para contornar ataques (p. ex., pass the hash). O **Privilege Service** também permite o acesso remoto seguro sem uma VPN. Ao mesmo tempo em que o tráfego de VPN pode ser seguro, ele também impõe outros riscos ao ambiente, ao permitir acesso mais amplo de usuários remotos para além dos servidores alvos nos que eles precisam fazer login.

Requisito 3: Proteja os dados de titulares de cartão armazenados

Nº	Requisito	Server Suite e Privilege Service
3.4.1	Se a criptografia do disco for usada (em vez de uma criptografia de banco de dados de nível de coluna ou arquivo), o acesso lógico deve ser gerenciado de forma separada e independente da autenticação de sistema operacional nativa e mecanismos de controle de acesso (por exemplo, ao não usar bancos de dados de conta de usuário local ou credenciais de login de rede gerais). Chaves de criptografia não devem ser associadas com contas de usuários	No ambiente Mac OSX, o **Server Suite** pode reforçar a criptografia completa do disco via FileVault 2. É possível fazer isso ao se definir uma Política de Grupo do Active Directory para o recurso. **O Server Suite** pode garantir/negar atividades privilegiadas, usando funções e direitos mantidos de forma independente do sistema operacional local no Active Directory

Requisito 4: Criptografe a transmissão de dados de titulares de cartão em redes abertas e públicas

Nº	Requisito	Server Suite e Privilege Service
4.1	Usar criptografia forte e protocolos de segurança (por exemplo, TLS, IPSEC, SSH, etc.) para proteger dados sensitivos do titular do cartão durante a transmissão em redes abertas, públicas	O **Server Suite Platinum Edition** oferece integridade com base em IPsec e serviços de confidencialidade no nível de rede para criptografar todas as comunicações entre uma aplicação no sistema e outras hospedagens remotas confiáveis. Uma vez que essa solução oferece serviços de criptografia no nível de rede, não há necessidade de modificar qualquer aplicação para oferecer suporte a esse nível de proteção de dados. Com o **Privilege Service**, todas as sessões de conta compartilhada privilegiadas para recursos são protegidas quanto a SSH ou RDP. Além disso, o **Privilege Service** oferece suporte a autenticação de dois fatores para usuários que fazem login no portal de **Privilege Service** portal para contornar ataques (p. ex., pass the hash)

Requisito 6: Desenvolva e mantenha sistemas e aplicativos seguros

Nº	Requisito	Server Suite e Privilege Service
6.3.1	Remover contas de aplicação de desenvolvimento, de teste e/ou padrão, IDs de usuários e senhas antes de aplicações se tornarem ativas ou serem liberadas para os consumidores.	A adição e remoção de contas específicas é tipicamente uma função de produtos de IAM de terceiros de fornecedores como IBM, CA Technologies e Oracle. Contudo, se essas contas estiverem sob gerenciamento do **Privilege Service**, podemos garantir que elas estão criptografadas e armazenadas com segurança e serão usadas apenas alinhadas com controles de acesso apropriados.
6.4	Seguir processos e procedimentos de controle de alteração para todas as mudanças em componentes de sistema	O **Server Suite** usa Zones para criar agrupamentos lógicos de sistemas que têm um conjunto distinto de usuários, administradores e políticas. Eles restringem os métodos de acesso e privilégios com base em cargo de trabalho. Essa restrição pode ser usada para fornecer separação entre máquinas de desenvolvimento, teste e produção e grupos de sistemas claramente separados e separação entre suas permissões. Esse modelo também trabalha bem para isolar sistemas de desenvolvimento de produção, ajudando a evitar o movimento de dados de teste para os sistemas de produção. O **Server Suite Platinum Edition** protege informação sensitiva, ao isolar e proteger de forma dinâmica sistemas de plataforma cruzada e permitir criptografia opcional de ponta a ponta de dados em movimento. Ele também aproveita o IPsec no modo de transporte para segurança de rede, que é aplicado a cada pacote individualmente, aproveitando as credenciais de PKI para estabelecer chaves de autenticação de sessão única para cada associação de segurança. O **Privilege Service** oferece suporte para um modelo de controle de acesso com base em função que garante que os usuários são capazes apenas de executar funções (login remoto, check-out de senha, permissões de concessão) apropriadas a sua função. Ele governa a autenticação do usuário a uma conta específica. Uma vez que o login é feito, o **Server Suite** pode então governar a autorização (p. ex., acesso específico).
6.4.2	Separação de tarefas entre desenvolvimento/teste e ambientes de produção	Conforme descrito em 6.4, acima, a tecnologia patenteada de Zone do **Server Suite** levam em conta a separação de tarefas por meio de restrição do acesso de administrador a recursos específicos. Isso permite que (p. ex.) um conjunto de servidores de desenvolvimento seja associado com administradores que podem fazer login nele, e, além disso, com um conjunto de direitos de acesso nesses sistemas. O mesmo pode ocorrer com grupos de recursos, como teste e produção.

Requisito 7: Restrinja o acesso aos dados de titulares de cartão com o princípio da necessidade de conhecer

Nº	Requisito	Server Suite e Privilege Service
7	Restrinja acesso aos dados de titulares de cartão com o princípio da necessidade de conhecer	**Server Suite** e **Privilege Service** implementam um modelo de controle de acesso de "privilégio mínimo" em que os usuários fazem login com suas próprias contas e solicitam de maneira explícita elevação de privilégio para executar distintas tarefas administrativas. Tais solicitações são garantidas ou negadas com base na necessidade de conhecer (ou seja, um modelo de controle de acesso com base em função) de forma central gerenciada por meio de Active Directory. Isso significa uma redução significativa da superfície de ameaça, ao evitar login direto e permitir que a maioria das contas privilegiadas compartilhadas seja desabilitada. Além disso, uma vez que as solicitações de acesso são feitas explicitamente em contraste com abordagens alternativas que interceptam cada ação de usuário única, política de verificação, e, em seguida, aplicam o resultado, o **Server Suite** tem impacto muito menor sobre os recursos de sistema e pode realizar registro de sessão de maneira seletiva em vez de capturar a sessão inteira, reduzindo sobrecarga de recursos e simplificando auditoria e atividades de investigação de segurança.
7.1	Limitar acesso aos recursos de computação e à informação de titular de cartão apenas aos indivíduos cujo trabalho exige tal acesso	O **Server Suite** utiliza Zones para controlar que usuários têm acesso garantido a sistemas específicos. Por padrão, o **Server Suite** reforça o modelo Zero Trust, ou seja, usuários do Active Directory não têm permissões para fazer login em qualquer sistema gerenciado por Server Suite. Contudo, ao adicionar um usuário a um Zone e criar um perfil UNIX para esse usuário no interior do Active Directory, o usuário terá acesso garantido aos sistemas de computadores que são membros do Zone ao qual o usuário foi adicionado. Isso resulta em uma configuração em que o **Server Suite** pode mostrar visualmente, assim como, informar sobre que usuários têm acesso aos sistemas específicos. Além disso, os grupos de Active Directory podem ser usados no interior de uma regra de configuração pam.allow no interior do **Server Suite** para restringir ainda mais que usuários no interior de um determinado Zone tenham permissão para fazer login em um sistema específico. Os parâmetros de configuração pam.allow e pam.deny podem ser usados para restringir o acesso a usuários individuais ou grupos de usuários. A Política de Grupo do Active Directory também pode controlar de forma centralizada essas regras. O Active Directory também fornece um parâmetro de configuração para cada usuário que permite que um administrador defina uma lista específica de computadores nos quais o usuário pode fazer login. Com o **Server Suite**, todos os sistemas não Windows têm uma conta de computador válida, que permite que os Administradores definam sistemas Windows e não Windows na lista de computadores com permissão. Essas regras de controle de acesso podem ser aplicadas para definir a política de controle de acesso exata necessária para o computador específico. O **Server Suite** oferece suporte para um modelo de controle de acesso com base em função que garante que os usuários são capazes apenas de executar funções (login remoto, check-out de senha, permissões de concessão) apropriadas a sua função. Ele governa a autenticação do usuário a uma conta específica. Uma vez que o login é feito, o **Server Suite** pode governar a autorização (p. ex., acesso específico). Por fim, o **Privilege Service** usa funções para governar que usuários têm permissão para fazer login em que recursos (servidores e dispositivos de redes)

Nº	Requisito	Server Suite e Privilege Service
7.2	Estabelecer um mecanismo para sistemas com usuários múltiplos que restringe acesso com base na necessidade de conhecer de um usuário e é definido como "negar tudo", a menos que haja permissão específica. Esse sistema de controle de acesso debe incluir o seguinte:	Tanto o **Server Suite** como o **Privilege Service** oferecem suporte a um modelo Zero Trust, de acordo com o qual os usuários não têm acesso aos recursos e não podem elevar privilégios elevados a menos que haja garantias explícitas. O **Server Suite** permite que os administradores gerenciem de forma centralizada um UNIX UID de usuário e associações ao grupo, que são, então, usadas pelo sistema de operação para controlar acesso de usuário a arquivos e aplicações específicas. A fim de oferecer controles mais rígidos em torno de operações privilegiadas, o **Server Suite** oferece uma Política de Grupo para permitir gerenciamento centralizado de permissões sudo para garantir que as permissões apropriadas sejam aplicadas a contas locais de uma maneira consistente em computadores em que esse privilégio deve ser garantido. O **Server Suite** estende essa funcionalidade para definir um conjunto de Funções que terá acesso específico garantido e direitos de comandos privilegiados. Essas Funções são definidas pelo fato de que o Active Directory permite que ambos os usuários e grupos do AD sejam atribuídos à Função, simplificando o gerenciamento contínuo. Essas ferramentas também servem para produzir uma trilha de auditoria de todas as operações privilegiadas, uma vez que sudo registrará todas as execuções de comando em que o comando su mais simples não fornece esse nível de visibilidade, nem permite que um usuário faça login como a conta raiz. O **Server Suite** também fornece um mecanismo para controlar a política de senha de conta de raiz por meio do Active Directory para proteger mais essas contas que, de outro modo, seriam capazes de obter acesso irrestrito a um sistema não Windows. Por padrão, o **Privilege Service** desabilita todo o acesso remoto a contas privilegiadas compartilhadas sob gerenciamento. O acesso deve ser garantido explicitamente por um administrador locatário
7.2.1	Cobertura de todos os componentes de sistema	**Server Suite** e **Privilege Service** governam acesso aos servidores, dispositivos de rede e aplicações/comandos específicos em servidores Windows, Unix e Linux no interior do escopo de PCI DSS, conforme descrito em 7.2, acima.
7.2.2	Atribuição de privilégios a indivíduos	Conforme as capacidades descritas em 7.2, acima, tanto **Server sSuite** como **Privilege Service** suportam mecanismos de acesso com base em função que governam login em recursos no interior de escopo bem como privilégios com base em funções que se equiparam a classificação de cargo e função, como descrito em 7.2, acima.
7.2.3	Conjunto "negar tudo" padrão.	Conforme as capacidades descritas em 7.2, acima, tanto o **Server Suite** como o **Privilege Service** oferecem suporte a um modelo Zero Trust, de acordo com o qual os usuários não têm acesso aos recursos e não podem elevar privilégios elevados até acessos e direitos explicitamente garantidos para fazer isso.

Requisito 8: Atribua um ID único a cada pessoa com acesso a um computador

Nº	Requisito	Server Suite e Privilege Service
8.1	Definir e implementar políticas e procedimentos para garantir gerenciamento de identificação de usuário adequado para usuários e administradores não consumidores em todos os componentes do sistema da seguinte maneira:	O **CSS** oferece suporte de gerenciamento de identidades do Windows, Unix, Linux e Mac de forma central no interior do Active Directory, permitindo que as empresas derrubem silos de identidade que resultam em contas invasoras e creep de privilégio. AD também é usado para aplicar funções e privilégios a usuários e computadores para garantir Controle de Acesso com base em Função consistente em todos os sistemas. Além disso, ele estende o modelo de política de grupo de AD para sistemas não Windows para gerenciamento mais fácil e mais consistente e aplicação abrangente de privilégios. Ver os detalhes adicionais abaixo
8.1.1	Atribuir um ID único a todos os usuários antes de permitir que eles acessem componentes de sistema ou dados do titular do cartão	Sistemas UNIX têm limitações como comprimento máximo do nome de login que tornam muito difícil para a equipe de TI estabelecer políticas que garantam que uma conta é única. Além disso, identificar a pessoa que de fato é proprietária de uma conta UNIX específica pode ser um desafio, graças às limitações de banco de dados de conta padrão que simplesmente não oferecem essa capacidade. Ao usar o Active Directory, todos os usuários têm uma única, em termos globais, conta de Active Directory que o **CSS** relaciona a cada perfil UNIX específico de usuário, o que elimina qualquer ambiguidade quanto a qual é o proprietário de uma conta UNIX específica ou arquivos criados por aquela conta. Em algumas implementações, grupos diferentes de sistemas UNIX podem ter um espaço de nome de UID local que se sobrepõe a outros grupos de sistemas no interior do ambiente. O **Zones** do **Server Suite** fornece a capacidade de permitir que um usuário tenha mais de um perfil UNIX para cada um desses grupos dos sistemas UNIX, eliminando, assim, qualquer ambiguidade de propriedade de conta ou arquivo, ao mesmo tempo em que a integridade de controle de acesso é preservada. Além disso, o **Privilege Service** reforça a singularidade dessas identidades - as identidades usadas para fazer login no próprio serviço do **Privilege** Service. Assim, todas as atividades privilegiadas (como o check-out de senha de conta privilegiada compartilhada) são relacionadas novamente a um único usuário
8.1.2	Adição de controle, exclusão e modificação de IDs, credenciais e outros objetos identificadores de usuário	Com o **Server Suite**, a administração de conta de usuário é centralmente gerenciada no interior do Active Directory, o que fornece um ambiente robusto para delegar a administração de contas do usuário à administração de Active Directory apropriado. O **Server Suite** estende essa administração delegada para oferecer suporte à delegação de gerenciamento de perfil UNIX ao administrador UNIX adequado sem exigir que os administradores do Active Directory garantam privilégios elevados no interior do Active Directory. O resultado é um ambiente em que os administradores UNIX têm permissão para garantir ou negar acesso aos sistemas UNIX, mas não têm o direito de criar um novo usuário no interior do Active Directory. Controles adicionais são fornecidos para evitar que os administradores do Active Directory criem um perfil UNIX, que poderia resultar em um usuário UNIX com privilégios elevados

Nº	Requisito	Server Suite e Privilege Service
8.1.3	Revogar imediatamente acesso a qualquer usuário desligado	Contas de usuários desligados são controladas por meio do Active Directory com o **Server Suite**. Até o desligamento, desativação ou exclusão da conta do Active Directory, o **Server Suite** recusa o login do usuário imediatamente. O **Privilege Service** pode aproveitar o Active Directory como seu armazenamento de usuário. Os usuários revogados no interior do Active Directory não poderão fazer login no **Privilege Service**. Se os usuários de portal do **Privilege Service** forem mantidos no Active Directory, LDAP ou no Centrify Cloud Directory, um consumidor pode aproveitar sua ferramenta IAM Provisioning para desprovisionar desses repositórios por meio (p. ex.) de LDAP ou SCIM
8.1.4	Remover/desabilitar contas de usuário inativas no interior de 90 dias	Contas de usuários inativas são controladas por meio do Active Directory com o **Server Suite**. O **Server Suite** atualiza de forma adequada o horário do último login para a conta do Active Directory do usuário, de forma que seja possível determinar que contas não foram usadas dentro de 90 dias. É decisão do administrador do domínio garantir de forma manual que os usuários inativos sejam removidos dele.
8.1.5	Gerenciar IDs usadas por fornecedores para acessar, oferecer suporte e manter componentes de sistema por meio de acesso remoto da seguinte maneira: Ativo apenas durante o período necessário e desativado quando não estiver em uso; Monitorado quando em uso	O Active Directory oferece tanto uma restrição de hora-do-dia quanto uma data de término de conta, que pode ser usada para restringir uma capacidade de conta a ser usada para login em todos os sistemas. O **Server Suite** também oferece um controle para permitir que o administrador UNIX habilite e desabilite de forma seletiva um perfil UNIX específico de usuário. Isso pode ser útil quando um usuário precisa de acesso periódico a um grupo de sistemas UNIX. Funções também podem ser definidas por um intervalo de tempo para garantir que elas só podem fornecer direitos de acesso específicos durante dias prescritos da semana e períodos do dia. O **Privilege Service** pode ter políticas habilitadas que governam usuários específicos, seu login no portal do **Privilege Service** (inclusive por meio da autenticação multifator) e os recursos que eles acessam. Podem ser estabelecidas políticas que desabilitam contas que não estão sendo usadas e as habilitam quando estão em uso
8.1.6	Limitar tentativas de acesso repetidas ao bloquear o ID de usuário depois de não mais do que seis tentativas	A política de bloqueio de conta é definida no interior do Active Directory e pode ser definida para bloquear contas depois de um número específico de tentativas de login inválidas. O **Server Suite** reforça essa política em sistemas não Windows. Uma vez que o **Privilege Service** gerencia senhas em nome de usuários, não há um número de tentativas de login inválidas. Alguns casos de uso (p. ex. "quebra de vidro") têm como resultado a revelação da senha a um administrador para login interativo. Nesse caso, a política de bloqueio de conta de AD pode ser definida de maneira que as contas sejam bloqueadas depois de um número específico de tentativas de login inválidas

Nº	Requisito	Server Suite e Privilege Service
8.1.7	Definir a duração do bloqueio para um mínimo de 30 minutos ou até que o administrador habilite o ID do usuário	A política de bloqueio de conta é definida no interior do Active Directory e pode ser definida para bloquear contas por um período específico, conforme necessário. O **Server Suite** reforça essa política em sistemas não Windows. Uma vez que o **Privilege Service** gerencia senhas em nome de usuários, não há um número de tentativas de login inválidas. Alguns casos de uso (p. ex. "quebra de vidro") têm como resultado a revelação da senha a um administrador para login interativo. Nesse caso, a política de bloqueio de conta de AD pode ser definida de maneira que a contas seja bloqueada por um período específico
8.1.8	Se a sessão estiver ociosa por mais de 15 minutos, exigir que o usuário faça nova autenticação para reativar o terminal ou sessão	A Centrify oferece distribuição binária de OpenSSH, configurada para usar as bibliotecas do **Server Suite** Kerberos para garantir que um usuário poderá obter acesso único de sign-on a um host remoto. O servidor OpenSSH pode ser configurado para exigir que uma sessão de usuário expire depois de um período específico ou depois de inatividade, como, por exemplo, 15 minutos. Depois de cada tempo limite, as credenciais de autenticação serão solicitadas ao usuário.
8.2.1	Usar criptografia forte, tornar todas as credenciais de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os componentes do sistema	**Server Suite**: Quando os sistemas são combinados com o Active Directory, toda autenticação será criptografada na transmissão e nenhuma senha percorrerá a rede com base no processo de autenticação Kerberos. O **Privilege Service** armazena senhas em um armazenamento por locatário seguro criptografado com chaves simétricas de bit AES256. Essas senhas são usadas em canais de comunicação criptografada, como HTTPS (para o usuário), SSH (para servidores *NIX) ou RDP (para servidores Windows).
8.2	Além de atribuir um ID único, garantir gerenciamento de autenticação de usuário para usuários e administradores não consumidores em todos os componentes do sistema ao empregar pelo menos um dos seguintes métodos para autenticar todos os usuários: • Algo que você sabe, como uma senha ou combinação de letra e número • Algo que você tem, como um dispositivo de token ou um smart card • Algo constitutivo, como biometria	Tanto o **Server Suite** quanto o **Privilege Service** oferecem suporte aos fatores listado como acréscimo a uma senha ou em lugar dela. As soluções oferecem suporte aos certificados MS Kerberos, X.509 e a smart cards, como PIV e CAC. É possível aplicar políticas para exigir um 2º fator de forma consiste ou solicitar um fator baseado em contexto, por exemplo, se o dispositivo móvel do usuário for registrado/confiável ou se o usuário estiver em uma rede interna.
8.2.1	Usar criptografia forte, tornar todas as credenciais de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os componentes do sistema.	O **Privilege Service** mantém senhas em um armazenamento seguro usando criptografia forte para torná-las ilegíveis. Senhas sempre são usadas em protocolos seguros.

Nº	Requisito	Server Suite e Privilege Service
8.2.2	Verificar identidade do usuário antes de modificar qualquer credencial de autenticação - por exemplo, realizando redefinições de senhas, fornecendo novos tokens ou gerando novas chaves	O **Server Suite** e o **Privilege Service** exigem que um usuário faça sua autenticação adequadamente antes de ter permissão para realizar essas mudanças. Senhas de conta compartilhadas privilegiadas são gerenciadas pelo **Privilege Service**, fará ciclos de senha em uma frequência programada e/ou quando um usuário voltar a verificar uma senha no **Privilege Service** depois do uso.
8.2.3	Senhas/frases devem estar de acordo com o seguinte: Exigir um comprimento mínimo de pelo menos sete caracteres; conter caracteres numéricos e alfabéticos Outra possibilidade é que as senhas/frases tenham complexidade e força pelo menos equivalente aos parâmetros especificados	A política de senha é definida no interior do Active Directory e pode ser definida para qualquer comprimento de senha e exigir construção com maiúsculas e minúsculas ou alfanumérica. O **Server Suite** permite que os sistemas não Windows usem senhas muito mais longas do que o comprimento com o qual o sistema conseguiria lidar, já que o Active Directory é usado para validar senhas de usuário. O **Privilege Service** gerencia senhas de conta privilegiadas compartilhadas em nome do usuário. Ele define essas senhas automaticamente para que elas sejam muito mais fortes e complexas do que os requisitos QOS típicos
8.2.4	Mudar as senhas/combinações de letra e número do usuário pelo menos a cada 90 dias	É possível definir a política de senha do Active Directory para que as senhas expirem e uma redefinição seja solicitada em um tempo limite de 90 dias ou menos. O **Server Suite** reforça essa política em sistemas não Windows.
8.2.5	Não permitir que uma nova senha/frase seja uma das últimas quatro senhas/frases usadas pelo usuário	A política de senha é definida no interior do Active Directory e pode ser definida para manter um histórico de senha e evitar que a senha seja usada novamente. O **Server Suite** reforça essa política em sistemas não Windows. O **Privilege Service** gerencia senhas de conta privilegiadas compartilhadas em nome do usuário. Ele define essas senhas para garantir que novas senhas não sejam iguais a uma das últimas quatro senhas usadas
8.2.6	Definir senhas/frases de primeiro uso e após o reinício para um valor único para cada usuário e mudar imediatamente após primeiro uso	O **Server Suite** obriga o usuário a mudar sua senha após o login inicial sempre que a conta do Active Directory estiver configurada para exigir que a senha seja alterada no próximo login. Essa opção normalmente é definida na criação de conta ou a qualquer momento que um administrador reinicie uma senha esquecida pelo usuário ou conta bloqueada. O **Privilege Service** pode reforçar esses procedimentos de senha para usuários que fazem login no portal do **Privilege Service**. A política de senha do Active Directory governa esse aspecto para senhas de conta privilegiada
8.3	Incorporar autenticação de dois fatores para acesso à rede remota com origem externa à rede, feito por pessoal (incluindo usuários e administradores) e todos os terceiros, (incluindo acesso de fornecedor para suporte ou manutenção).	Esse requisito deve se atendido por sistemas de controle de acesso à rede antes do acesso do usuário a um sistema UNIX ou Linux. Uma vez que o usuário for autenticado de forma adequada na rede remota, o acesso ao sistema é tratado como se o usuário estivesse na rede local. A política do **Privilege Service** pode reforçar o uso de autenticação de dois fatores para login de portal. Após o login a um servidor remoto ser realizado, a política do **Server Suite** pode reforçar a autenticação de dois fatores para elevação privilegiada

Nº	Requisito	Server Suite e Privilege Service
8.4	Documentar e comunicar procedimentos e políticas de autenticação para todos os usuários, incluindo: Orientação sobre seleção de credenciais fortes de autenticação; orientações sobre como os usuários devem proteger suas credenciais de autenticação, instruções para que senhas usadas anteriormente não sejam reutilizadas, instruções para mudar senhas se houver qualquer suspeita de que a senha pode ter sido comprometida	Os administradores precisam informar os usuários sobre as políticas e procedimentos de senha. Contudo, é importante notar que com o **Server Suite**, essas políticas e procedimentos são reforçados de forma idêntica tanto nos sistemas Windows como UNIX e Linux. Como o **Privilege Service** é definido para controlar e gerenciar senhas de conta privilegiada, os usuários não estão no controle; assim, políticas de senhas não são relevantes
8.5	Não utilizar IDs e senhas genéricos, compartilhados ou de grupo ou outros métodos de autenticação como estes: IDs de usuário são desabilitadas ou removidas; IDs de usuário não existem para a administração do sistema e outras funções críticas, IDs de usuário genéricas ou compartilhada não são usadas para administrar qualquer componente do sistema	O **Server Suite** cria um ambiente que permite que os usuários possam fazer login com sua própria conta única do Active Directory e solicitar elevação de privilégio de forma explícita para executar comandos privilegiados. O **Server Suite** garante ou nega essas solicitações com base em um mecanismo de Controle de Acesso Baseado em Função. Assim, em condições ideais, IDs de usuário genéricas e compartilhadas estão desabilitadas e não podem ser usadas imediatamente para login. Essa abordagem também garante confiabilidade plena, já que as ações privilegiadas estão associadas a um único indivíduo e não a uma entidade anônima, como "raiz" ou "administrador". Podem ocorrer situações em que não há outra escolha a não ser habilitar contas compartilhadas e permitir login direto (por exemplo, na atualização de um sistema operacional). O **Privilege Service** pode ser usado nesse caso para assumir o controle da senha e registrar automaticamente o usuário sem revelar essa senha. É possível fazer um ciclo da senha quando o trabalho estiver completo. Relatórios sobre IDs de usuário do Active Directory permitirão que o administrador veja se há contas genéricas ou compartilhadas. Se existir de fato alguma conta genérica ou compartilhada, o relatório mostrará as funções e privilégios associados. O **Privilege Service** também pode controlar que IDs de usuários genéricas ou compartilhadas estão disponíveis para login remoto, p. ex., por TI externo.
8.6	Nos casos em que outros mecanismos de autenticação são usados (por exemplo, tokens de segurança físicos ou lógicos, smart cards, certificados etc.) o uso desses mecanismos deve ser atribuído da seguinte maneira: Mecanismos de autenticação devem ser atribuídos a uma conta individual e não devem ser compartilhados entre contas múltiplas; controles físicos e/ou lógicos devem estar em vigor para garantir que apenas a conta selecionada pode usar esse mecanismo para obter acesso	A Centrify oferece suporte a uma gama de mecanismos de autenticação, incluindo Kerberos, X.509 e cartões PIV/CAC. Com o **Server Suite**, a Centrify associa credenciais de login a uma única pessoa com base em sua entrada única do Active Directory. Mecanismos de autenticação e acesso garantem que apenas usuários autorizados podem obter acesso aos recursos que os usuários têm autorização de usar por tais meios.

Nº	Requisito	Server Suite e Privilege Service
8.7	Todos os acessos a qualquer banco de dados que contém dados do titular do cartão (incluindo acesso por aplicações, administradores e todos os outros usuários) são restringidos da seguinte maneira: Todos os acessos, consultas e ações do usuário relacionados à base de dados são realizados por meio de métodos programáticos; apenas administradores de banco de dados têm a capacidade de acessar ou consultar banco de dados de forma direta; IDS de aplicação para aplicações de banco de dados podem ser usadas apenas pelas aplicações (e não por usuários individuais ou outros processos que não são aplicações).	A Centrify fornece ferramentas de configuração e plug-ins conforme necessário para integrar a autenticação de bancos de dados Oracle, DB2, Sybase e Informix com o Active Directory, de forma a permitir contas centralizadas e reforço de política de senha

Requisito 10: Acompanhe e monitore todo o acesso aos recursos da rede e aos dados de titulares de cartão

Nº	Requisito	Server Suite e Privilege Service
10.1	Estabelecer um processo para relacionar todo acesso aos componentes do sistema (especialmente aqueles feitos com privilégios administrativos, como, por exemplo, raiz) a um usuário individual	O **Server Suite** estabelece um contexto de usuário válido para a conta UNIX, que é relacionada diretamente a uma conta do Active Directory para garantir que todas as trilhas de auditoria possam ter origem em uma pessoa. O **Server Suite** trabalha com um modelo de privilégio mínimo em que cada usuário faz login com um ID pessoal, inequívoco. Todas as atividades são relacionadas novamente ao usuário, garantindo confiabilidade. Todos os usuários do **Privilege Service** fazem login com seu próprio ID individual. Com isso, as atividades são plenamente confiáveis. Para atividades privilegiadas, o **Server Suite Enterprise Edition** e o **Privilege Service** podem registrar sessões para revisão visual detalhada de todas as atividades. Além disso, o registro de sessão mantém um registro forense visual de todas as atividades de sessão remotas
10.2.1	Verificar se todo acesso individual aos dados do titular do cartão é registrado	O **Server Suite** permite rastrear toda autenticação de usuário e operações de gerenciamento de conta por meio de registros mantidos no controlador de domínio do Active Directory que realiza a ação. Os Controladores de Domínio registrarão todas as tentativas de login, sejam elas bem-sucedidas ou inválidas. O **Server Suite Enterprise Edition** cria e armazena de forma centralizada um registro de todas as ações do usuário realizadas no sistema para usuários do Active Directory, bem como de contas locais. O registro contém todas as ações realizadas independentemente do nível de privilégio do usuário, incluindo qualquer acesso de usuário de trilhas de auditoria ou registros e objetos de nível de sistema.

Nº	Requisito	Server Suite e Privilege Service
10.2.1	Verificar se todo acesso individual aos dados do titular do cartão é registrado	Como os registros de auditoria são armazenados no interior de um sistema central que não está localizado no sistema auditado, a segurança é aprimorada com uma segunda máquina que também reforça os controles de acesso em todos os acessos privilegiados de banco de dado. Para atividades privilegiadas, o **Server Suite Enterprise Edition** pode registrar sessões para revisão detalhada de todas as atividades na tela. O **Privilege Service** auditará e registrará as atividades de sessão de registro para todas as sessões iniciadas por meio de jump box (ou seja, não se audita "quebra de vidro"). Ele também auditará atividades realizadas no nível de portal - login, check-out de senha, solicitação de login remoto etc.
10.2.2	Verificar se todas as ações realizadas por qualquer indivíduo com privilégios de raiz ou administrativos são registradas	A fim de oferecer controles mais rígidos em torno de operações privilegiadas, o **Server Suite** oferece uma Política de Grupo para permitir gerenciamento centralizado de permissões sudo para garantir que as permissões apropriadas sejam aplicadas a contas locais de uma maneira consistente em computadores em que esse privilégio deve ser garantido. O **Server Suite** estende essa funcionalidade para definir um conjunto de Funções que terá acesso específico garantido e direitos de comandos privilegiados. Essas Funções são definidas pelo fato de que o Active Directory permite que ambos os usuários e grupos do AD sejam atribuídos à Função, simplificando o gerenciamento contínuo. Essas ferramentas também servem para produzir uma trilha de auditoria de todas as operações privilegiadas, uma vez que sudo registrará todas as execuções de comando em que o comando su mais simples não fornece esse nível de visibilidade, nem permite que um usuário faça login como a conta raiz. O **Server Suite** também fornece um mecanismo para controlar a política de senha de conta de raiz por meio do Active Directory para proteger mais essas contas que, de outro modo, seriam capazes de obter acesso irrestrito a um sistema não Windows. O **Server Suite Enterprise Edition** cria e armazena de forma centralizada um registro de todas as ações do usuário realizadas no sistema para usuários do Active Directory, bem como de contas locais. O registro contém todas as ações realizadas independentemente do nível de privilégio do usuário, incluindo qualquer acesso de usuário de trilhas de auditoria ou registros e objetos de nível de sistema. Como os registros de auditoria são armazenados no interior de um sistema central que não está localizado no sistema auditado, a segurança é aprimorada com uma segunda máquina que também reforça os controles de acesso em todos os acessos privilegiados de banco de dado. Para atividades privilegiadas, o **Server Suite Enterprise Edition** pode registrar sessões para revisão detalhada de todas as atividades na tela. O **Privilege Service** auditará e registrará as atividades de sessão de registro para todas as sessões iniciadas por meio de jump box (ou seja, não se audita "quebra de vidro"). Ele também auditará atividades realizadas no nível de portal - login, check-out de senha, solicitação de login remoto etc.

Nº	Requisito	Server Suite e Privilege Service
10.2.3	Verificar se o acesso a todas as trilhas de auditoria é registrado	Como acontece com arquivos ou bancos de dados que contêm informações de auditoria, o acesso a trilhas de auditoria pode ser protegido como qualquer outra fonte de sistema que usa acesso de privilégio mínimo, controles de acesso com base em função e elevação de privilégio. No interior das UIs administrativas do **Server Suite Enterprise Edition**, o acesso a dados de trilhas de auditoria por meio de mecanismo de consulta e relatórios integrados pode ser governado por funções e por tais atividades registradas. No interior das UIs do **Privilege Service** , o acesso a dados de trilhas de auditoria é governado por funções e por tais atividades registradas.
10.2.4	Verificar se tentativas de acesso lógico inválidas são registradas	O Active Directory e o Linux registrarão tentativas de autenticação inválidas. O Active Directory registra logins de estações de trabalho inválidos ou solicitações de entrada Kerberos a sistemas não autorizados. O Linux registra tentativas de login inválidas realizadas de forma interativa. O **Privilege Service** auditará atividades realizadas no nível de portal - login, check-out de senha, solicitação de login remoto etc.
10.2.5	Uso e mudanças de mecanismos de identificação e autenticação — incluindo, mas não se limitando a, criação de novas contas e elevação de privilégios — e todas as mudanças, adições ou exclusões em contas com privilégios raiz ou administrativos	O **Server Suite** define um conjunto de Funções que terá acesso específico garantido e direitos de comandos privilegiados. Essas Funções são definidas pelo fato de que o Active Directory permite que ambos os usuários e grupos do Active Directory sejam atribuídos à Função, simplificando o gerenciamento contínuo. Essas ferramentas também servem para produzir uma trilha de auditoria de todas as operações privilegiadas, uma vez que sudo registrará todas as execuções de comando em que o comando su mais simples não fornece esse nível de visibilidade, nem permite que um usuário faça login como a conta raiz. O **Server Suite** também fornece um mecanismo para controlar a política de senha de conta de raiz por meio do Active Directory para proteger mais essas contas que, de outro modo, seriam capazes de obter acesso irrestrito a um sistema não Windows. O **Server Suite** Enterprise Edition cria e armazena de forma centralizada um registro de todas as ações do usuário realizadas no sistema tanto para usuários do Active Directory como para contas locais. O registro contém todas as ações realizadas independentemente do nível de privilégio do usuário, incluindo qualquer acesso de usuário de trilhas de auditoria ou registros e objetos de nível de sistema. Como os registros de auditoria são armazenados no interior de um sistema central que não está localizado no sistema auditado, a segurança é aprimorada com uma segunda máquina que também reforça os controles de acesso em todos os acessos privilegiados de banco de dado. Para atividades privilegiadas, o **Server Suite Enterprise Edition** pode registrar sessões para revisão detalhada de todas as atividades na tela. O **Privilege Service** auditará atividades realizadas no nível de portal - login, check-out de senha, solicitação de login remoto e mudanças administrativas, como a criação ou mudança de contas.
10.2.6	Inicialização, interrupção ou pausa de registros de auditoria	O **Server Suite Enterprise Edition** monitora seu próprio registro de auditoria por meio de pulsação para o banco de dados de registro de auditoria central

Nº	Requisito	Server Suite e Privilege Service
10.2.7	Criação e exclusão de objetos de nível de sistema	Todas as atividades do usuário que são registradas pelo **Server Suite Enterprise Edition** incluem a identidade do usuário que realiza a ação. Como o modelo da Centrify é um modelo de privilégio mínimo, em que identidades únicas são usadas para fazer login em contraste com contas compartilhadas, essas entradas de registro levam de volta ao usuário real em vez de levar ao usuário anônimo. O **Privilege Service** inclui o nome do usuário que realiza as operações de nível de sistema em objetos
10.3	Registrar pelo menos as seguintes entradas de trilha de auditoria para todos os componentes do sistema para cada evento: Identificação de uso; tipo de evento; data e horário; indicação de sucesso ou falha; origem do evento; identidade ou nome dos dados, sistema, componente ou recurso afetados	As soluções da Centrify mantêm trilhas de auditoria (p. ex., syslog, Log de Eventos do Windows e seu próprio banco de dados de auditoria), bem como os registros de sessão das atividades privilegiadas. A Centrify captura todos os dados identificados em 10.3.1 por meio de 10.3.6.
10.4	Usando tecnologia de sincronização de data/hora, sincronizar todos os relógios e horários críticos do sistema e garantir que o que segue é implementado para aquisição, distribuição e horário de armazenamento	O **Server Suite** configura e reforça automaticamente a Política de Sincronização do Horário definido no interior do Grupo de Política do Active Directory Group em todos os sistemas UNIX e Linux que são relacionados ao Active Directory. Essa sincronização de horário será realizada com a infraestrutura do controlador de domínio do Active Directory, que deve ser configurado para sincronização de horário com uma camada 1 clock
10.5	Assegurar trilhas de auditoria de modo que elas não possam ser alteradas	O **Server Suite Enterprise Edition** tem sido planejado para prevenir visualização ou manipulação não autorizada dos registros de sessão do usuário. Essa ação é executada pelo daemon da auditoria, conforme transmite de forma segura o registro de auditoria para um coletor centralizado que armazena os dados em um repositório do SQL Server sob políticas restritas de controle de acesso. Os registros de auditoria não são tipicamente armazenados de forma local, a menos que a conectividade da rede com um coletor esteja desativada, no ponto em que a rede armazenará em cache de forma local e enviará para armazenamento para o coletor quando a conectividade da rede é restaurada. O console de **Auditoria do Server Suite Enterprise Edition** permitirá apenas que os auditores autorizados visualizem as sessões do usuário que estava registrado no uso das credenciais do Active Directory para a estação de trabalho que executa o console. Esse console é projetado para controlar que pessoal tem acesso aos registrados centralizados. O Servidor do Microsoft SQL é usado para armazenar e gerenciar dados de auditoria de modo que dados estabelecidos podem ser protegidos com controles rigorosos de acesso e que esse acesso possa ser registrado
10.6	Revisar registros e eventos de segurança para todos os componentes do sistema para identificar anomalias ou atividades suspeitas	O **Server Suite Enterprise Edition** armazena os dados de auditoria em um texto sem formatação, de formato não proprietário de forma que outras ferramentas como os Serviços de Relatório SQL possam ser usados para analisar os dados e gerar alertas, conforme necessário
10.7	Reter histórico de trilha de auditoria por pelo menos um ano, com um mínimo de três meses imediatamente disponíveis para análise (por exemplo, backup de formulário online, arquivado ou restaurável).	Backup de dados padrão e restaurar procedimentos podem ser usados para gerenciar os dados de registro que o **Server Suite Enterprise Edition** armazena no interior do repositório do SQL Server para habilitar a política de backup que está em conformidade com esse requisito

Requisito 11: Teste regularmente os sistemas e processos de segurança

Nº	Requisito	Server Suite e Privilege Service
11.4	Usar técnicas de detecção de intrusão e/ou prevenção de intrusão para detectar e/ou prevenir intrusões na rede. Monitorar todo o tráfego no perímetro do ambiente de dados do titular do cartão, bem como os pontos críticos nesse ambiente e alertar o pessoal quanto a comprometimentos suspeitos. Manter todos os mecanismos, linhas de base e assinaturas de detecção de intrusão e prevenção atualizados	Embora o **Server Suite Platinum Edition** não seja projetado especificamente para prevenção de intrusão, ele pode ser configurado conforme descrito acima para permitir que apenas sistemas confiáveis específicos se comuniquem, prevenindo, assim, intrusos oriundos de acesso de sistemas de PCI.
11.5	Empregar um mecanismo de detecção de mudança (por exemplo, ferramentas de monitoramento de integridade de arquivo) para avisar o pessoal sobre modificação não autorizada (incluindo, mudanças, adições e exclusões) de arquivos de sistema críticos, arquivos de configuração ou arquivos de conteúdo; e configurar o software para realizar comparações de arquivos críticos pelo menos semanalmente.	A Centrify tem visibilidade única de usuários e seus direitos ("quem tem acesso a quê"), bem como de suas atividades ("quem fez o quê"). Ela pode pré-correlacionar esses dados e torná-los disponíveis para uma solução do cliente de Gerenciamento e Correlação de Eventos de Segurança (SIEM) existente a fim de que os dados sejam usados como parte de um mecanismo de detecção de mudança.
12	Manter uma política que trate da segurança das informações para todo o pessoal	A Centrify aproveita o AD para definir de maneira central e gerenciar identidades de usuário, recursos e políticas de forma consistente em todas as plataformas Windows e não Windows. Ela também registra e grava atividades de sessão privilegiadas. Desse modo, esse é um importante feed em um programa de segurança de informação e avaliação de risco do cliente.
12.2	Implementar um processo de avaliação de risco que: • é realizado pelo menos uma vez ao ano e a cada mudança significativa no ambiente (por exemplo, aquisição, fusão, realocação etc.), • identifica ativos, ameaças e vulnerabilidades críticos e • resulta em análise de risco formal e documentada	O **Server Suite Platinum Edition** e o **Privilege Service** incluem registro e auditoria baseados em evento, assim como registro de sessão visual com reprodução de vídeo. A transcrição de sessão isola atividades e recomendações específicas inseridas para ajudar sas empresas a simplificar suas avaliações e investigações de risco, permitindo que ela enfoque rapidamente atividades privilegiadas nas quais tentativas de violações de política foram realizadas. O **Server Suite** ajuda ainda na avaliação de riscos e nas verificações de pontos de segurança com a opção de registrar seletivamente atividades de sessão associadas apenas com a execução de comandos privilegiados, em vez de sessões de login inteiras.

SANTA CLARA, CALIFÓRNIA	+ 1 (669) 444 5200
EMEA	+44 (0) 1344 317950
ÁSIA PACÍFICO	+61 1300 795 789
BRASIL	+55 11 3958 4876
AMÉRICA LATINA	+1 305 900 5354
E-MAIL	sales@centrify.com
WEB	www.centrify.com