Segurança do macOS

Descrição geral para o departamento de TI

A Apple concebeu a plataforma macOS a pensar na segurança, com uma abordagem integrada ao hardware, software e serviços que simplifica a configuração, implementação e gestão. O macOS inclui as principais tecnologias de segurança de que os profissionais de TI necessitam para proteger os dados empresariais e efetuar a integração em ambientes de rede empresarial seguros. A Apple também aplicou normas para garantir a conformidade com as certificações de segurança mais recentes. Esta descrição geral explica de forma breve algumas dessas funcionalidades.

Este documento está organizado de acordo com as seguintes áreas de tópicos:

- **Segurança do sistema:** o software integrado e seguro que está na base do macOS.
- **Encriptação e proteção de dados:** a arquitetura e design que protegem os dados do utilizador em caso de perda ou roubo do dispositivo.
- **Segurança das apps:** os sistemas que protegem o Mac do malware e permitem que as apps sejam utilizadas de forma segura, sem comprometer a integridade da plataforma.
- **Autenticação e assinaturas digitais:** os mecanismos incluídos no macOS para a gestão de credenciais e compatibilidade com tecnologias de referência no setor, como cartões e S/MIME.
- **Segurança de rede:** protocolos de rede de referência no setor que permitem a autenticação segura e encriptação dos dados em trânsito.
- **Controlos do dispositivo:** métodos que permitem a gestão de dispositivos Apple, impedem a utilização não autorizada e ativam a eliminação remota dos dados em caso de perda ou roubo do dispositivo.

Para mais informações sobre a implementação e gestão do macOS, consulte o Manual de referência de implementação do macOS em help.apple.com/deployment/macos.

Para mais informações sobre as funcionalidades de segurança de serviços da Apple não descritos neste documento, consulte o "Guia de segurança do iOS" em www.apple.com/business/docs/iOS_Security_Guide.pdf.

Segurança do sistema

A segurança do sistema macOS foi concebida de forma a proteger o software e o hardware nos componentes principais de todos os Mac. Esta arquitetura é essencial para a segurança do macOS, e nunca interfere com a facilidade de utilização dos dispositivos.

UNIX

O kernel do macOS, que é o núcleo do sistema operativo, baseia-se no Berkeley Software Distribution (BSD) e microkernel Mach. O BSD fornece serviços básicos de sistema de ficheiros e rede, um esquema de identificação de utilizadores e grupos, e muitas outras capacidades fundamentais. O BSD também aplica restrições de acesso a ficheiros e recursos do sistema, com base em ID de utilizadores e grupos.

O Mach oferece gestão de memória, controlo de thread, abstração de hardware e comunicação interprocessos. As portas do Mach representam tarefas e outros recursos, e o Mach controla o acesso às portas determinando que tarefas lhes podem enviar mensagens. As políticas de segurança do BSD e as autorizações de acesso do Mach constituem a base essencial da segurança do macOS, e são fundamentais para garantir a segurança local.

A segurança do kernel é essencial para a proteção de todo o sistema operativo. A assinatura de código protege as extensões de kernel e kernel de outras empresas, bem como outras bibliotecas de sistema e executáveis desenvolvidos pela Apple.

Modelo de autorização do utilizador

Um aspeto importante da segurança do Mac é a aprovação ou recusa de permissões de acesso (também conhecidas como direitos de acesso). Uma autorização é a capacidade de efetuar uma operação específica, como obter acesso aos dados ou executar código. As autorizações são concedidas ao nível das pastas, pastas subordinadas, ficheiros e apps, bem como para dados específicos em ficheiros, capacidades de apps e funções administrativas. As assinaturas digitais identificam os direitos de acesso das apps e componentes do sistema.

O macOS controla as autorizações a vários níveis, incluindo os componentes Mach e BSD do kernel. Para controlar as autorizações para apps na rede, o macOS utiliza protocolos de rede.

Controlos de acesso obrigatórios

O macOS também utiliza controlos de acesso obrigatórios, políticas que definem restrições de segurança criadas pelo programador e que não podem ser ignoradas. Esta abordagem difere dos controlos de acesso opcionais, que permitem aos utilizadores ignorar as políticas de segurança de acordo com as suas preferências. Os controlos de acesso obrigatórios, que não são visíveis para os utilizadores, são a tecnologia subjacente que ajuda a ativar várias funcionalidades importantes, incluindo o sistema Sandbox, controlos parentais, preferências geridas, extensões e Proteção da integridade do sistema.

Proteção da integridade do sistema

O OS X 10.11 ou posterior inclui proteção ao nível do sistema, denominada Proteção de integridade do sistema, que restringe componentes para o modo só de leitura em localizações críticas e específicas do sistema de ficheiros, de forma a evitar que código nocivo os execute ou modifique. A Proteção de integridade do sistema é uma definição específica de computador que é ativada por predefinição ao atualizar para o OS X 10.11; a sua desativação remove a proteção de todas as partições no dispositivo de armazenamento físico. O macOS aplica esta política de segurança a todos os processos executados no sistema, independentemente de serem executados no modo sandbox ou com privilégios de administrador.

Para mais informações sobre estas áreas só de leitura do sistema de ficheiros, consulte o artigo do Suporte Apple "Acerca da Proteção de integridade do sistema no Mac" em support.apple.com/HT204899.

Extensões do kernel

O macOS fornece um mecanismo de extensão do kernel para permitir o carregamento dinâmico de código no kernel sem necessidade de voltar a compilar ou ligar. Uma vez que estas extensões do kernel (KEXT) fornecem modularidade e carregamento dinâmico, são uma escolha natural para qualquer serviço relativamente restrito que requeira acesso a interfaces do kernel internas, como controladores de dispositivos de hardware ou apps VPN.

Para aumentar a segurança do Mac, é necessário o consentimento do utilizador para carregar extensões de kernel instaladas durante ou após a instalação do macOS High Sierra. Esta ação é conhecida como Carregamento de extensões do kernel aprovado pelo utilizador. Qualquer utilizador pode aprovar uma extensão do kernel, mesmo que não tenha privilégios administrativos.

As extensões do kernel não requerem autorização se:

- Foram instaladas no Mac antes da atualização para o macOS High Sierra.
- Substituírem extensões previamente aprovadas.
- For permitido o carregamento sem o consentimento do utilizador através do comando `spctl` disponível no arranque a partir da partição de recuperação do macOS.
- For permitido o carregamento através da configuração da gestão de dispositivos móveis (MDM). A partir do macOS High Sierra 10.13.2, pode utilizar a MDM para especificar uma lista de extensões de kernel que são carregadas sem o consentimento do utilizador. Esta opção requer um Mac com o macOS High Sierra 10.13.2 que esteja registado na MDM através do Programa de registo de dispositivos (DEP) ou através do registo na MDM aprovado pelo utilizador.

Para mais informações sobre as extensões do kernel, consulte o artigo do Suporte Apple "Preparação para alterações nas extensões do kernel no macOS High Sierra" em support.apple.com/HT208019.

Palavra-passe do firmware

O macOS permite a utilização de uma palavra-passe para impedir alterações acidentais das definições de firmware num sistema específico. Esta palavra-passe do firmware é utilizada para evitar o seguinte:

- Arranque a partir de um volume de sistema não autorizado
- Alteração do processo de arranque, como o arranque no modo de utilizador único
- Acesso não autorizado à Recuperação do macOS
- Acesso direto à memória (DMA) através de interfaces como Thunderbolt
- Modo de disco de destino, que requer DMA

Nota: o processador T2 da Apple no iMac Pro impede que os utilizadores reponham a palavra-passe do firmware, mesmo se obtiverem acesso físico ao Mac. Num Mac sem o processador T2, devem ser tomadas precauções adicionais para impedir que os utilizadores tenham acesso físico aos componentes internos do Mac.

Recuperação da internet

Quando não conseguem efetuar o arranque a partir do sistema de recuperação integrado, os computadores Mac tentam automaticamente efetuar o arranque a partir da Recuperação do macOS na internet. Nesta situação, surge um globo em rotação no ecrã, em vez do logótipo da Apple. Com a recuperação da internet, os utilizadores podem reinstalar a versão mais recente do macOS ou a versão fornecida com o Mac.

As atualizações do macOS são distribuídas através da App Store e executadas pelo macOS Installer, que utiliza as assinaturas de código para garantir a integridade e autenticidade do instalador e dos respetivos pacotes antes da instalação. Da mesma forma, o serviço de recuperação da internet é a fonte autorizada para o sistema operativo fornecido com um Mac específico.

Para mais informações sobre a Recuperação do macOS, consulte o artigo do Suporte Apple "Acerca da Recuperação do macOS" em support.apple.com/HT201314.

Encriptação e proteção de dados

Sistema de ficheiros Apple

O Apple File System (APFS) é um sistema de ficheiros novo e moderno para o macOS, iOS, tvOS e watchOS. Otimizado para armazenamento Flash/SSD, inclui encriptação forte, metadados de cópia em gravação, partilha de espaço, clonagem de ficheiros e diretórios, instantâneos, rápido dimensionamento de diretório, primitivos atómicos de armazenamento seguro e básicos de sistema de ficheiros melhorados, bem como um design de cópia em gravação exclusivo que utiliza coalescência de entrada/saída para proporcionar o máximo desempenho garantindo a fiabilidade dos dados.

O APFS atribui espaço em disco a pedido. Quando um contentor do APFS tem vários volumes, o espaço livre no contentor é partilhado e pode ser atribuído a qualquer dos volumes individuais, consoante necessário. Cada volume utiliza apenas parte do contentor global, como tal o espaço disponível é o tamanho total do contentor, subtraindo o espaço utilizado em todos os volumes no contentor.

Para o macOS High Sierra, um contentor APFS válido deve conter pelo menos três volumes, sendo que os dois primeiros são ocultados do utilizador:

- Volume de pré-arranque: contém dados necessários para o arranque de cada volume de sistema no contentor.
- Volume de recuperação: contém o disco de recuperação.
- Volume de sistema: contém o macOS e a pasta do utilizador.

FileVault

Todos os Mac oferecem uma capacidade de encriptação integrada, denominada FileVault, para proteger todos os dados inativos. O FileVault utiliza encriptação de dados XTS-AES-128 para proteger os dados num Mac inativo. Tal pode ser aplicado à proteção total de volumes, a dispositivos de armazenamento interno e amovíveis. Se um utilizador introduzir um ID Apple e palavra-passe durante o Assistente de Configuração, o assistente sugere a ativação do FileVault e o armazenamento da chave de recuperação no iCloud.

Um utilizador que ative o FileVault num Mac deve fornecer credenciais válidas antes de continuar o processo de arranque e para obter acesso a modos de

arranque especializados, como o modo de disco de destino. Sem credenciais de início de sessão válidas ou uma chave de recuperação, todo o volume permanece encriptado e protegido contra o acesso não autorizado, mesmo que o dispositivo de armazenamento físico seja removido e ligado a outro computador.

Para proteger dados numa configuração empresarial, o departamento de TI deve definir e implementar políticas de configuração do FileVault através da MDM. As empresas têm várias opções para gerir volumes encriptados, incluindo chaves de recuperação institucionais, chaves de recuperação pessoais (que podem, opcionalmente, ser armazenadas na MDM como depósito), ou uma combinação de ambas. A rotação de chaves também pode ser definida como uma política na MDM.

Imagens de disco encriptadas

No macOS, as imagens de disco encriptadas funcionam como contentores seguros em que os utilizadores podem armazenar ou transferir documentos sensíveis e outros ficheiros. As imagens de disco encriptadas são criadas utilizando o Utilitário de Discos, que se encontra em /Aplicações/Utilitários/. As imagens de disco podem ser encriptadas utilizando encriptação AES de 128 ou 256 bits. Uma vez que uma imagem de disco montada é tratada como um volume local ligado a um Mac, os utilizadores podem copiar, mover e abrir ficheiros e pastas nela armazenados. Como acontece com o FileVault, os conteúdos de uma imagem de disco são encriptados e desencriptados em tempo real. Com imagens de disco encriptadas, os utilizadores podem trocar documentos, ficheiros e pastas em segurança guardando uma imagem de disco encriptada em suportes amovíveis, enviando-a como um anexo de email ou armazenando-a num servidor remoto.

Certificações ISO 27001 e 27018

A Apple recebeu a certificação ISO 27001 e ISO 27018 para o sistema de gestão da segurança da informação (ISMS) para a infraestrutura, desenvolvimento e operações compatíveis com estes produtos e serviços: Apple School Manager, iCloud, iMessage, FaceTime, ID Apple geridos e iTunes U, em conformidade com a Declaração de Aplicabilidade v2.1, datada de 11 de julho de 2017. A conformidade da Apple com a norma ISO foi certificada pela British Standards Institution (BSI). Para ver os certificados de conformidade ISO 27001 e ISO 27018, consulte o website da BSI:

www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=apple&licencenumber=IS+649475

www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=Apple&licencenumber=PII%20673269

Validação criptográfica (FIPS 140-2)

Os módulos criptográficos no macOS foram validados repetidamente para conformidade com as normas de processamento de informações federais dos EUA (FIPS - Federal Information Processing Standards) 140-2 Nível 1 após cada lançamento desde o OS X 10.6. Como acontece em cada grande lançamento, a Apple envia os módulos ao CMVP para revalidação quando o sistema operativo do Mac é lançado. Este programa valida a integridade das operações criptográficas para apps Apple e de outras empresas que utilizem adequadamente os serviços criptográficos e os algoritmos aprovados do

macOS. Todos os certificados de validação de conformidade da Apple com FIPS 140-2 podem ser encontrados na página do fornecedor CMVP. O CMVP mantém o estado de validação dos módulos criptográficos em duas listas separadas, consoante o estado atual, em csrc.nist.gov/groups/STM/cmvp/inprocess.html.

Certificação de critérios comuns (ISO 15408)

A Apple obteve anteriormente certificações para o macOS no âmbito do programa de Certificação de critérios comuns e está novamente a envolver-se numa avaliação do macOS High Sierra relativamente ao Perfil de proteção do sistema operativo (PP_OSv4.1). A Apple continua a avaliar e procurar certificações de versões novas e atualizadas dos Perfis de proteção colaborativos (cPP) disponíveis atualmente. A Apple teve um papel ativo na Comunidade técnica internacional (ITC) para o desenvolvimento de cPP que focam a avaliação de tecnologia de segurança móvel essencial.

Certificações de segurança, programas e orientação

A Apple trabalhou com governos em todo o mundo para desenvolver guias com instruções e recomendações para a manutenção de um ambiente mais seguro, também denominado "fortalecimento de dispositivos" para ambientes de alto risco. Estes guias fornecem informações definidas e aprovadas sobre como configurar e utilizar funcionalidades integradas no macOS para proteção avançada.

Para conhecer as informações mais recentes sobre certificações, validações e diretrizes de segurança para macOS, consulte o artigo do Suporte Apple "Certificações, validações e diretrizes de segurança dos produtos para macOS" em support.apple.com/HT201159.

Segurança de apps

O macOS inclui tecnologias integradas para garantir que apenas são instaladas apps fiáveis e ajudar a proteger contra malware. Para garantir que apps legítimas não são adulteradas, o macOS também inclui uma abordagem em camadas à proteção de tempo de execução de apps e à assinatura de apps.

Gatekeeper

Para controlar as fontes a partir das quais é possível instalar apps, o macOS fornece uma funcionalidade denominada Gatekeeper. O Gatekeeper permite aos utilizadores e empresas definir um nível de segurança necessário para instalar apps.

Com a definição do Gatekeeper mais segura, os utilizadores apenas podem instalar apps assinadas da App Store. A predefinição permite aos utilizadores instalar apps da App Store e apps com uma assinatura de Developer ID válida. Esta assinatura indica que as apps foram assinadas por um certificado emitido pela Apple e que não foram alteradas desde então. O Gatekeeper também pode ser totalmente desativado através de um comando Terminal, se necessário.

Além disso, o Gatekeeper aplica a aleatorização dos caminhos em alguns casos, incluindo quando as apps são iniciadas diretamente a partir de uma imagem de disco não assinada ou da localização para a qual foram descarregadas e automaticamente desarquivadas. A aleatorização dos caminhos torna as apps disponíveis a partir de uma localização só de leitura não especificada no sistema de ficheiros antes da execução. Tal evita que as apps acedam a código ou conteúdos utilizando caminhos relativos, mas também as impede de autoatualizar se forem iniciadas a partir desta localização só de leitura. A utilização do Finder para mover uma app, por exemplo, para a pasta Aplicações significa que a aleatorização dos caminhos não será mais aplicada.

O principal benefício do modelo de proteção predefinido é que oferece uma ampla proteção do ecossistema. Caso um autor de malware consiga roubar ou obter de outra forma a capacidade de assinatura de Developer ID e utilizá-la para distribuir malware, a Apple consegue responder rapidamente revogando o certificado de assinatura. Tal vai impedir a difusão do malware. Essas proteções reduzem o modelo económico da maioria das campanhas de malware no Mac e proporcionam uma ampla proteção a todos os utilizadores.

Os utilizadores podem ignorar temporariamente estas definições para instalar uma app. As empresas podem utilizar a sua solução MDM para estabelecer e implementar definições do Gatekeeper, bem como adicionar certificados à política de confiança do macOS para avaliar a assinatura de código.

XProtect

O macOS inclui tecnologia integrada para a deteção de malware baseada em assinatura. A Apple monitoriza as novas infeções e estirpes de malware e atualiza automaticamente as assinaturas do XProtect, independentemente das atualizações do sistema, para ajudar a defender os sistemas Mac contra infeções de malware. O XProtect deteta e bloqueia automaticamente a instalação de malware conhecido.

Ferramenta de remoção de malware

Caso o malware consiga aceder a um Mac, o macOS também inclui tecnologia para remediar infeções. Além da monitorização da atividade de malware no ecossistema ser capaz de revogar uma Developer ID (se aplicável) e emitir

atualizações do XProtect, a Apple também emite atualizações para o macOS para remover malware de quaisquer sistemas infetados que estejam configurados para receber atualizações de segurança automáticas. Quando a ferramenta de remoção de malware receber informação atualizada, o malware será removido após o reinício seguinte. A ferramenta de remoção de malware não reinicia o Mac automaticamente.

Atualizações de segurança automáticas

A Apple emite atualizações para o XProtect e para a ferramenta de remoção de malware automaticamente. Por predefinição, o macOS verifica estas atualizações diariamente. Para mais informações sobre atualizações de segurança automáticas, consulte o artigo do Suporte Apple "Mac App Store: atualizações de segurança automáticas" em support.apple.com/HT204536.

Proteção de tempo de execução

Os ficheiros de sistema, recursos e o kernel estão protegidos do espaço de apps de um utilizador. Todas as apps da App Store estão em sandbox para restringir o acesso aos dados armazenados por outras apps. Se uma app da App Store precisar de aceder a dados de outra app, apenas pode fazê-lo utilizando as API e os serviços fornecidos pelo macOS.

Assinatura de código de apps obrigatória

Todas as apps da App Store são assinadas pela Apple para garantir que não foram adulteradas ou modificadas. A Apple assina todas as apps fornecidas com dispositivos Apple. Muitas apps distribuídas fora da App Store são assinadas pelo programador utilizando um certificado de Developer ID emitido pela Apple (combinado com uma chave privada) para execução nas predefinições do Gatekeeper.

As apps externas à App Store, normalmente, são igualmente assinadas com um certificado de programador emitido pela Apple. Desta forma, é possível validar que a app é genuína e não foi adulterada. As apps desenvolvidas internamente também devem ser assinadas com um Developer ID emitido pela Apple, para que seja possível validar a sua integridade.

Os controlos de acesso obrigatórios (MAC - Mandatory Access Controls) requerem a assinatura de código para ativar direitos protegidos pelo sistema. Por exemplo, as apps que requeiram acesso através da firewall devem ser assinadas por código com o direito MAC adequado.

Autenticação e assinatura digital

Para o armazenamento conveniente e seguro das credenciais e identidades digitais dos utilizadores, o macOS inclui o Porta-chaves e outras ferramentas para suportar tecnologias de autenticação e assinatura digital, como cartões inteligentes e S/MIME.

Arquitetura do Porta-chaves

O macOS oferece um repositório denominado Porta-chaves, que armazena de forma conveniente e segura nomes de utilizadores e palavras-passe, incluindo identidades digitais, chaves de encriptação e notas seguras. Para aceder basta abrir a app Acesso a Porta-chaves em /Aplicações/Utilitários/. A utilização do porta-chaves elimina a necessidade de ter de utilizar, ou até de se lembrar, das credenciais para cada recurso. É criado um porta-chaves predefinido inicial

para cada utilizador Mac, mas os utilizadores podem criar outros porta-chaves para efeitos específicos.

Para além dos porta-chaves de utilizadores, o macOS possui vários porta-chaves ao nível do sistema, que mantêm os ativos de autenticação não específicos do utilizador, tais como as credenciais de rede e as identidades da infraestrutura de chave pública (PKI). Um desses porta-chaves, System Roots, é imutável e armazena certificados da autoridade de certificação de raiz (CA) de PKI da Internet para facilitar tarefas comuns como serviços bancários online e comércio eletrónico. Pode também implementar certificados CA aprovisionados internamente em computadores Mac geridos para ajudar na validação de locais e serviços internos.

Estrutura de autenticação segura

Os dados do Porta-chaves são divididos e protegidos com listas de controlo de acesso (ACL), por isso, as credenciais guardadas por apps de terceiros não podem ser acedidas por apps com identidades diferentes, a não ser que o utilizador as aprove explicitamente. Esta proteção concede o mecanismo para proteger as credenciais de autenticação nos dispositivos Apple numa grande variedade de apps e serviços na sua organização.

Touch ID

Os sistemas Mac com sensor Touch ID podem ser desbloqueados utilizando uma impressão digital. O Touch ID não substitui a necessidade de uma palavra-passe, que continua a ser necessária para iniciar sessão ao ligar, reiniciar ou terminar sessão no Mac. Depois de iniciarem sessão, os utilizadores podem proceder rapidamente à autenticação com o Touch ID sempre que lhes seja solicitada uma palavra-passe.

Os utilizadores também podem utilizar o Touch ID para desbloquear notas protegidas por palavra-passe na app Notas, no painel de Palavras-passe de preferências do Safari e muitos painéis de preferências nas Preferências do Sistema. Para reforçar a segurança, os utilizadores têm de introduzir uma palavra-passe em vez de utilizar o Touch ID para desbloquear o painel de Segurança e Privacidade nas Preferências do Sistema. Se o FileVault estiver ativado, os utilizadores também têm de introduzir uma palavra-passe para gerir as preferências de Utilizadores e Grupos. Vários utilizadores que iniciem sessão no mesmo Mac podem utilizar o Touch ID para alternar entre contas.

Para mais informações sobre o Touch ID e a respetiva segurança, consulte o artigo do Suporte Apple "Acerca da tecnologia de segurança avançada do Touch ID" em support.apple.com/HT204587.

Desbloqueio automático com Apple Watch

Os utilizadores com Apple Watch podem utilizá-lo para desbloquear automaticamente o Mac. As funcionalidades Bluetooth Low Energy (BLE) e Wi-Fi peer-to-peer permitem ao Apple Watch desbloquear com segurança um Mac depois de assegurar a proximidade entre os dispositivos. Isso requer uma conta iCloud com a autenticação de dois fatores (TFA) configurada.

Para detalhes sobre o protocolo, bem como para mais informações sobre as funcionalidades Continuidade e Handoff, consulte o "Guia de segurança do iOS" em www.apple.com/business/docs/iOS_Security_Guide.pdf.

Cartões inteligentes

O macOS Sierra e superior inclui compatibilidade de raiz com cartões de verificação de identidade pessoal (PIV). Estes cartões são amplamente utilizados em organizações comerciais e governamentais para TFA, assinatura digital e encriptação.

Os cartões inteligentes incluem uma ou mais identidades digitais com um par de chaves públicas e privadas e um certificado associado. Desbloquear um cartão inteligente com o número de identificação pessoal (PIN) concede o acesso às chaves privadas utilizadas para operações de autenticação, encriptação e assinatura. O certificado determina para o que uma chave pode ser utilizada, que atributos estão associados à mesma e se a esta foi validada (assinada) por uma CA.

Os cartões inteligentes podem ser utilizados para a autenticação de dois fatores. Os dois fatores necessários para desbloquear um cartão são "algo que você tem" (o cartão) e "algo que você sabe" (o PIN). O macOS Sierra e superior inclui compatibilidade de raiz com autenticação de janela de início de sessão de cartão inteligente e autenticação de certificado de cliente para websites no Safari. Também é compatível com a autenticação Kerberos utilizando pares de chaves (PKINIT) para início de sessão único em serviços compatíveis com Kerberos.

Para mais informações sobre a implementação de cartão inteligente com macOS, consulte o Manual de referência de Implementação do macOS em help.apple.com/deployment/macos.

Assinatura digital e encriptação

Na app Mail, os utilizadores podem enviar mensagens assinadas digitalmente e encriptadas. O Mail descobre automaticamente endereços de e-mail sensíveis a maiúsculas e minúsculas RFC 822 adequados de sujeitos ou nomes alternativos de sujeitos em certificados de assinatura digital e encriptação em tokens PIV anexados em cartões inteligentes compatíveis. Se uma conta de e-mail configurada corresponder a um endereço de e-mail num certificado de assinatura digital ou encriptação num token PIV anexado, o Mail apresenta automaticamente o botão de assinatura na barra de ferramentas de uma janela de mensagem nova. Se o Mail tiver o certificado de encriptação de e-mail do destinatário ou puder descobri-lo na Lista de Endereços Global do Microsoft Exchange (GAL), abre-se um ícone de desbloqueio na barra de ferramentas de mensagem nova. Um ícone de bloqueio indica que a mensagem será enviada encriptada com a chave pública do destinatário.

S/MIME por mensagem

O macOS é compatível com S/MIME por mensagem. Isto significa que os utilizadores S/MIME podem optar por assinar e encriptar sempre as mensagens por predefinição ou por assinar e encriptar seletivamente mensagens individuais.

As identidades utilizadas com S/MIME podem ser entregues aos dispositivos Apple utilizando um perfil de configuração, uma solução MDM, o protocolo SCEP (Simple Certificate Enrollment Protocol) ou a autoridade Microsoft Active Directory Certificate Authority.

Segurança da rede

Para além das proteções integradas que a Apple utiliza para proteger os dados guardados nos computadores Mac, existem muitas medidas de segurança de rede que as organizações podem adotar para manter as informações seguras quando entram e saem do Mac.

Os utilizadores móveis têm de ser capazes de aceder a redes empresariais a partir de qualquer local do mundo, por isso é importante assegurar que estão autorizados e que os respetivos dados estão protegidos durante a transmissão. O macOS utiliza e concede o acesso a programadores relativamente a protocolos de rede padrão para comunicações autenticadas, autorizadas e encriptadas. Para alcançar estes objetivos de segurança, o macOS integra tecnologias comprovadas e os mais recentes padrões para ligações de redes de dados Wi-Fi.

TLS

O macOS é compatível com Transport Layer Security (TLS 1.0, TLS 1.1 e TLS 1.2) e DTLS. É compatível com AES-128 e AES-256, e prefere cipher suites com perfect forward secrecy. O Safari, Calendário, Mail e outras apps da Internet utilizam automaticamente este protocolo para ativar um canal de comunicação encriptado entre o dispositivo e os serviços de rede.

APIs de alto nível (tais como CFNetwork) fazem com que seja mais fácil para os programadores adotar TLS nas respetivas apps, ao passo que APIs de baixo nível (tais como SecureTransport) concedem um controlo fino. CFNetwork desativa SSLv3, e as apps que utilizam WebKit (como o Safari) estão proibidas de realizar uma ligação SSLv3.

Relativamente a macOS High Sierra e iOS 11, os certificados SHA-1 já não são permitidos para as ligações TLS a não ser que o utilizador os considere seguros. Os certificados com chaves RSA inferiores a 2048 bits também não são permitidos. O cipher suite simétrico RC4 é evitado no macOS Sierra e iOS 10. Por predefinição, os clientes ou servidores TLS implementados com APIs SecureTransport não têm RC4 cipher suites ativados e não podem ligar-se quando o RC4 é o único cipher suite disponível. Para serem mais seguros, os serviços ou as apps que exijam RC4 devem ser atualizados para utilizar cipher suites modernos e seguros.

App Transport Security

O App Transport Security oferece requisitos de ligação predefinidos para que as apps adiram às melhores práticas para ligações seguras ao utilizar APIs NSURLConnection, CFURL ou NSURLSession. Por predefinição, o App Transport Security limita a seleção cipher para incluir apenas suites que ofereçam forward secrecy, especificamente ECDHE_ECDSA_AES e ECDHE_RSA_AES no modo GCM ou CBC. As apps podem desativar o requisito forward secrecy numa base por domínio, sendo que RSA_AES é adicionado ao conjunto de ciphers disponível.

Os servidores têm de ser compatíveis com TLS 1.2 e forward secrecy, e os certificados têm de ser válidos e assinados utilizando SHA-256 ou superior com uma chave RSA de 2048 bits no mínimo ou chave de curva elítica de 256 bits.

As ligações de rede que não correspondam a estes requisitos irão falhar, a não ser que a app se sobreponha ao App Transport Security. Os certificados inválidos resultam sempre numa falha e na ausência de ligação. O App

Transport Security é automaticamente aplicado às apps compiladas para macOS 10.11 ou posterior.

VPN

Geralmente, os serviços de rede seguros como rede privada virtual (VPN) requerem uma configuração mínima para funcionar com macOS.
Os computadores Mac funcionam com servidores VPN compatíveis com os seguintes protocolos e métodos de autenticação:

- IKEv2/IPSec com autenticação por segredo partilhado, certificados RSA, certificados ECDSA, EAP-MSCHAPv2 ou EAP-TLS
- SSL VPN utilizando a app cliente adequada da App Store
- Cisco IPSec com autenticação do utilizador através de palavra-passe, RSA SecurID ou CRYPTOCard, e autenticação de máquina através de segredo partilhado e certificados
- L2TP/IPSec com autenticação do utilizador através de palavra-passe MS-CHAPV2, RSA SecurID ou CRYPTOCard, e autenticação de máquina através de segredo partilhado

Para além das soluções VPN de terceiros, o macOS é compatível com o seguinte:

- **VPN On Demand** para redes que utilizam a autenticação baseada em certificado. As políticas de TI especificam que domínios requerem uma ligação VPN utilizando um perfil de configuração VPN.
- **VPN por app** para facilitar ligações VPN numa base muito mais granular. A MDM pode especificar uma ligação para cada app gerida e domínios específicos no Safari. Isso ajuda a garantir que os dados seguros vão sempre para e da rede empresarial e que o mesmo não se passa com os dados pessoais do utilizador.

Wi-Fi

O macOS é compatível com protocolos Wi-Fi padrão da indústria, incluindo WPA2 Enterprise, para conceder o acesso autenticado a redes empresariais sem fios. WPA2 Enterprise utiliza encriptação AES de 128 bits, concedendo aos utilizadores o mais elevado nível de segurança de que os respetivos dados permanecem protegidos ao enviar e receber comunicações através de uma ligação de rede Wi-Fi. Com compatibilidade com 802.1X, os computadores Mac podem ser integrados numa grande variedade de ambientes de autenticação RADIUS. Os métodos para autenticação sem fios 802.1X incluem EAP-TLS, EAP-TTLS, EAP-FAST, EAP-AKA, PEAPv0, PEAPv1 e LEAP.

A autenticação WPA/WPA2 Enterprise também pode ser utilizada na janela de início de sessão do macOS para que o utilizador inicie sessão para autenticar a rede.

O Assistente de configuração do macOS é compatível com a autenticação 802.1X com credenciais de nome de utilizador e palavra-passe utilizando TTLS ou PEAP.

Firewall

O macOS inclui uma firewall integrada para proteger o Mac relativamente a ataques de acesso à rede e negação de serviço. É compatível com as configurações seguintes:

- Bloquear todas as ligações de entrada, independentemente da app

- Permitir automaticamente o software integrado para receber ligações de entrada
- Permitir automaticamente o software transferido e assinado para receber ligações de entrada
- Adicionar ou negar o acesso com base nas apps especificadas pelo utilizador
- Impedir que o Mac responda a pedidos de sondagem ICMP e portscan

Single Sign-On

O macOS é compatível com autenticação para redes empresariais utilizando o Kerberos. As apps podem utilizar o Kerberos para autenticar os utilizadores em serviços que estão autorizados a aceder. O Kerberos também pode ser utilizado para uma grande variedade de atividades de rede, de sessões seguras do Safari e autenticação de sistema de ficheiros de rede a apps de terceiros.
A autenticação baseada em certificado (PKINIT) é compatível, embora seja necessária a adoção da app de um API de programação.

Os tokens GSS-API SPNEGO e o protocolo de negociação HTTP funcionam com gateways de autenticação baseados no Kerberos e sistemas de Autenticação Integrada do Windows compatíveis com tickets Kerberos.
A compatibilidade com o Kerberos baseia-se no projeto de fonte aberta Heimdal.

São compatíveis os seguintes tipos de encriptação:

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Para configurar o Kerberos, adquira tickets com Ticket Viewer, inicie sessão num domínio Windows Active Directory ou utilize a ferramenta de linha de comandos `kinit`.

Segurança AirDrop

Os computadores Mac compatíveis com AirDrop utilizam a tecnologia BLE e Wi-Fi peer-to-peer criada pela Apple para enviar ficheiros e informações para dispositivos nas proximidades, incluindo dispositivos iOS compatíveis com AirDrop com iOS 7 ou posterior. O rádio Wi-Fi é utilizado para comunicar diretamente entre dispositivos sem utilizar qualquer ligação à Internet ou ponto de acesso Wi-Fi. Esta ligação é encriptada com TLS.

Para mais informações sobre AirDrop, segurança do AirDrop e outros serviços Apple, consulte a secção "Network Security" (Segurança de rede) do "Guia de segurança do iOS" em www.apple.com/business/docs/iOS_Security_Guide.pdf.

Controlos do dispositivo

O macOS é compatível com políticas e configurações de segurança flexíveis e fáceis de implementar e gerir. Isto permite às organizações proteger informações empresariais e assegurar que os funcionários correspondem aos requisitos da empresa, mesmo que utilizem os próprios computadores, por exemplo, no âmbito de um programa "trazer o próprio dispositivo" (BYOD).

As organizações podem utilizar recursos como a proteção por palavra-passe, perfis de configuração e soluções MDM de terceiros para gerir conjuntos de

dispositivos e manter os dados empresariais seguros, mesmo quando os funcionários acederem aos dados nos computadores Mac pessoais.

Proteção por palavra-passe

Nos computadores Mac com Touch ID, a extensão mínima da palavra-passe corresponde a oito caracteres. É recomendável utilizar palavra-passe longas e complexas, uma vez que são mais difíceis de descobrir ou atacar.

Os administradores podem implementar palavras-passe complexas e outras políticas utilizando MDM ou solicitando aos utilizadores que instalem manualmente os perfis de configuração. É necessária uma palavra-passe de administrador para instalação da carga útil da política de palavra-passe do macOS.

Para detalhes sobre cada política disponível nas definições MDM, consulte help.apple.com/deployment/mdm/#/mdm4D6A472A.

Para detalhes de programação sobre cada política, consulte a Referência do Perfil de Configuração em developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef.

Implementação da configuração

Um perfil de configuração consiste num ficheiro XML que permite a um administrador distribuir informações de configuração a computadores Mac. Se o utilizador eliminar um perfil de configuração, todas as definições constantes do perfil também são removidas. Os administradores podem implementar as definições ligando as políticas ao acesso Wi-Fi e de dados. Por exemplo, um perfil de configuração que conceda uma configuração de e-mail também pode especificar uma política de palavra-passe do dispositivo. Um utilizador não poderá aceder ao mail se a palavra-passe não corresponder aos requisitos do administrador.

Um perfil de configuração do macOS contém várias definições que podem ser especificadas, incluindo:

- Políticas de código
- Restrições relativas às funcionalidades do dispositivo (por exemplo desativação da câmara)
- Definições Wi-Fi ou VPN
- Definições do servidor Mail ou Exchange
- Definições do serviço de diretório LDAP
- Definições da firewall
- Credenciais e chaves
- Atualizações de software

Para uma lista atualizada de perfis, consulte o Manual de Referência sobre o Perfil de Configuração em help.apple.com/deployment/mdm/#/mdm5370d089.

Os perfis de configuração podem ser assinados e encriptados para validar as respetivas origens, assegurar a integridade e proteger o conteúdo. Para além disso, os perfis de configuração também podem ser bloqueados para um Mac para impedir totalmente a respetiva remoção ou para a permitir apenas mediante palavra-passe. Os perfis de configuração que incluam um Mac numa solução MDM podem ser removidos, mas ao fazê-lo, também são removidas informações de configuração gerida, dados e apps.

Os utilizadores podem instalar perfis de configuração transferidos do Safari, enviados numa mensagem de e-mail ou utilizando uma solução MDM. Quando um utilizador configura um Mac em DEP ou Apple School Manager, o computador transfere e instala automaticamente um perfil para o registo MDM.

MDM

A compatibilidade do macOS com a MDM permite às empresas configurar e gerir de forma segura implementações dimensionáveis do Mac, iPhone, iPad e Apple TV. Estão integradas capacidades da MDM em tecnologias do macOS existentes, como perfis de configuração, registo sem fios e o serviço de notificações Push da Apple (APN). Por exemplo, as APN são utilizadas para ativar o dispositivo, de forma a poder comunicar diretamente com a solução de MDM através de uma ligação segura. As APN não transmitem informações confidenciais ou sujeitas a direitos de propriedade.

Com a MDM, os departamentos de TI podem registar computadores Mac num ambiente empresarial, configurar e atualizar definições sem fios, monitorizar a conformidade com as políticas da empresa e até bloquear ou apagar remotamente os dados de computadores Mac geridos.

Registo de dispositivos

O registo de dispositivos, que faz parte do Apple School Manager e dos Programas de implementação Apple, consiste numa forma rápida e simples de implementar computadores Mac que uma organização adquiriu diretamente à Apple ou através de Apple Authorized Resellers participantes.

As organizações podem registar automaticamente computadores na MDM sem terem de tocar fisicamente ou preparar os computadores antes de os utilizadores terem acesso aos mesmos. Após o registo, os administradores iniciam sessão no website do programa e ligam-no à respetiva solução MDM. Em seguida, os computadores adquiridos podem ser automaticamente atribuídos através de uma solução de MDM. Após o registo de um Mac, todas as configurações, restrições ou controlos especificados pela MDM são automaticamente instalados. Todas as comunicações entre os computadores e os servidores Apple são encriptadas em trânsito com HTTPS (SSL).

Para simplificar o processo de configuração, podem eliminar-se passos específicos do Assistente de configuração, para que os utilizadores possam começar a trabalhar rapidamente. Os administradores também podem controlar se o utilizador pode ou não remover o perfil MDM do computador e assegurar que foram implementadas restrições ao dispositivo desde o início. Quando o computador é retirado da caixa e ativado, é registado na solução MDM da organização e todas as definições de gestão, apps e livros são instalados. Nota: o registo de dispositivos não está disponível em todos os países ou regiões.

Para mais informações relacionadas com empresas, consulte a Ajuda dos Programas de implementação Apple em help.apple.com/deployment/business. Para mais informações relacionadas com a educação, consulte a Ajuda do Apple School Manager em help.apple.com/schoolmanager.

Restrições

Os administradores podem ativar, ou, em alguns casos, desativar restrições para impedir que os utilizadores acedam a uma app, serviço ou função específica do dispositivo. As restrições são enviadas para os dispositivos numa

carga útil de Restrições num perfil de configuração. Podem ser aplicadas restrições a dispositivos macOS, iOS e tvOS.

Pode consultar uma lista atualizada de restrições disponíveis para gestores de TI em: help.apple.com/deployment/mdm/#/mdm2pHf95672

Eliminação remota e bloqueio remoto

Os computadores Mac podem ser eliminados remotamente por um administrador ou utilizador. A eliminação remota instantânea apenas está disponível se o Mac tiver o FileVault ativado. Quando é desencadeado um comando de eliminação remota através de MDM ou iCloud, o computador envia um reconhecimento e efetua a eliminação. Com o bloqueio remoto, a MDM exige a aplicação de um código de seis dígitos ao Mac, bloqueando qualquer utilizador até que o código seja introduzido.

Privacidade

A Apple está convicta de que a privacidade é um direito fundamental do ser humano, por isso todos os produtos Apple são concebidos para, sempre que possível, utilizar o processamento no próprio dispositivo, limitar a recolha e utilização de dados, conceder transparência e controlo relativamente às informações e confiar numa base de segurança sólida.

A Apple dispõe de diversos controlos e opções integrados que permitem aos utilizadores do macOS decidir como e quando as apps utilizam as informações, bem como que informações estão a ser utilizadas. Para mais informações, consulte www.apple.com/pt/privacy.