Como permitir o acesso do drive USB
sem comprometer a segurança do Endpoint

Introdução

Em janeiro de 1996, a especificação do USB 1.0 oficial no lançamento foi anunciar uma nova era de uniformidade, conveniência e versatilidade para fornecedores de dispositivos periféricos e também para os usuários finais. 27 anos depois, ele mantém a compatibilidade de antigamente com cada revisão, e o USB resiste como um marco fundamental da interface de hardware do computador desde servidores até smartphones.

A simplicidade de plug-and-play do USB e velocidades ainda mais rápidas fizeram o armazenamento portátil USB evoluir como um dos grandes vencedores. Mesmo assim, tal conveniência tem um porém quando se trata de segurança de dados. No mundo de hoje, sem o uso das ferramentas corretas como segurança de endpoint em computadores host e práticas de segurança de dados apropriadas, os usuários com atitudes mais descuidadas em relação ao uso de armazenamento portátil USB deixam a si mesmos e a outros expostos a possíveis violações de dados que podem custar caro para o usuário final e ainda comprometer toda uma empresa ou governo.

Além disso, para proteger o ambiente do host, o drive USB também deve ser protegido com proteção por senha e criptografia de hardware no dispositivo. Isso oferece a defesa mais sólida contra invasões. Nós vamos abordar algumas das melhores práticas para usar drives USB de forma mais segura junto a um olhar mais profundo sobre drives USB em geral.

Enquanto uma abordagem combinada é o ideal, é a solidez da criptografia e os componentes de hardware do drive USB em si que são de importância primordial. Estes beneficiam os setores de finanças, saúde, manufatura e militar. Eles também desempenham um papel no trabalho remoto onde o acesso à rede é indisponível, vulnerável ou inviável.

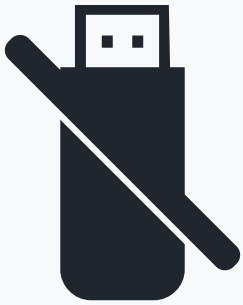
Os drives USB criptografados com base em hardware estão disponíveis com diferentes classificações de certificação enquanto fornecem uma gama de recursos de segurança. Ao examinar seus atributos e oportunidades de customização, suas adequações como soluções independentes são também ilustradas ao proteger seus lugares de todas as formas de ambientes sensíveis.

Autoridade de entrada: O armazenamento USB atende ao software de prevenção de perda de dados de gestão de Endpoint

Por décadas, aplicativos antivírus e antimalware ofereceram proteção nos níveis mais fundamentais - escaneando automaticamente downloads e dispositivos anexados e relatando ou agindo sobre conteúdos suspeitos. A proteção pelo software Next Generation Anti-Virus (NGAV) leva isso mais além. Ao invés de confiar apenas em um banco de dados de assinaturas de vírus atualizado continuamente, o NGAV adiciona aprendizado de máquina e recursos de detecção comportamental que podem identificar e mitigar ameaças desconhecidas.

Mas essa não é a única arma do arsenal, e para aqueles que querem proteção à prova de bala de periféricos de usuários e ainda mais, o software de Prevenção de Perda de Dados (DLP) de gestão de Endpoint fornece os meios para negar qualquer tipo de acesso às portas USB e outros pontos de acesso.

A atitude de segurança de 'bloquear todas as portas pode certamente eliminar riscos e, em algumas circunstâncias, pode ser desejável, mas tal política pode frequentemente provar ser um instrumento muito brusco com consequências indesejáveis.



Ainda assim, alguns administradores de TI preferem recusar solicitações para abrir portas USB em máquinas de usuários, já que fazer isso nesses endpoints permitirá acesso direto através do firewall da empresa. Tal precaução é compreensível mas quando se trata de permitir acesso para armazenamento USB, prover este privilégio não precisa ser uma dor de cabeça enorme na questão da segurança se certos pré-requisitos forem observados.

Uma exigência essencial é um conjunto de aplicativos de gestão de endpoint que inclui escaneamento para detecção de ameaças em soluções de antivírus e antimalware, bem como gestão e monitoramento centralizados de todos os endpoints do usuário.

De forma geral, essa abordagem direta aparece sob vários aspectos em soluções unificadas de fornecedores populares como McAfee MVision, Sophos Intercept X, Symantec Endpoint Security, Trend Micro Smart Protection e WinMagic SecureDoc, entre outros.

Aperfeiçoamentos em listas de permissões

Quando se trata de segurança para dispositivos de armazenamento USB, o método implementado depende do nível de proteção exigido. Uma abordagem simples porém eficaz é autorizar dispositivos de armazenamento USB a utilizarem seus respectivos valores de Vendor Identifier (VID) e Product Identifier (PID). Um aspecto sobre todos os periféricos USB é que cada fabricante tem uma única VID, mas a PID muda para cada novo produto lançado.

Para incluir na lista de permissões, usar a VID de um fabricante sozinha seria muito amplo para ser seguro, já que todo dispositivo USB que ele já produziu seria permitido. A PID oferece mais refinamento e exigências que apenas um modelo específico ter acesso ao sistema host.

Mesmo sendo um progresso, ainda não é o ideal. Dispositivos de armazenamento USB são muito populares por permitir que o usuário adquira seu próprio dispositivo combinando com os modelos autorizados. Mantendo isso em mente, a Kingston Technology oferece uma solução sob medida para endurecer a segurança de dispositivos de armazenamento USB.

Disponível através de seu programa de customização, perfis de PID personalizados e específicos para uma organização podem ser criados e aplicados à uma gama de pendrives USB criptografados. Empresas implementando dispositivos incluindo um identificador de produto personalizado não se beneficiam apenas da lista de permissões simplificada, mas também de uma segurança mais reforçada. Sem combinar a PID customizada, mesmo dispositivos aparentemente idênticos comprados independentemente por funcionários terão o acesso negado.

Enquanto o uso de PIDs customizadas permitirá que os administradores de TI tragam novos dispositivos de armazenamento USB de forma rápida e fácil, uma alternativa mais granular é usar números de série individuais de

dispositivos que estão incluídos na maioria dos drives USB criptografados da Kingston. Este acordo requer que cada número de série único de dispositivo seja registrado com a suíte de gestão de endpoint. Inicialmente, isso envolverá o processamento pela equipe de TI e nesse caso a Kingston pode fornecer uma lista de números de série com cada pedido - eles serão sempre alfanuméricos e não sequenciais. Escolher esse método permite políticas muito mais flexíveis com base em propriedade do drive individual com o bônus de um rastreamento preciso de procedência de dispositivos, o que pode ser inestimável em cenários forenses de TI. Alguns drives da Kingston incluem um número de série e um código de barras no invólucro para escaneamento eletrônico e outros drives podem ser customizados para adicionar um código de barras e um número de série no invólucro para negócios, esses itens podem ser usados para rastreamento do drive.

Por padrão, os sistemas de gestão de endpoint fornecem acesso à VID/PID para bloqueio de portas e lista de permissões. O que a Kingston oferece é uma forma mais versátil de aproveitar estas características para permitir políticas mais flexíveis e creativas para facilitar o uso de dispositivo de armazenamento USB. Ao estabelecer um método de identificação apropriado, uma atitude de 'Bloquear todas as portas não é apenas simples demais, mas também se torna desnecessária.

Soluções compatíveis e seguras para usuários remotos

Quando se trata de segurança, a permissão de dispositivos trata apenas da metade do problema, ou colocando de outra forma, metade da solução.

A conveniência e simplicidade dos dispositivos de armazenamento USB os tornam indispensáveis em muitos negócios e instituições onde a portabilidade é a chave para transferências de dados sem atritos. Na maioria dos ambientes, por razões de conformidade e higiene de TI, é necessário equipar os funcionários com dispositivos USB criptografados para tais tarefas. Ao utilizar uma combinação de proteção por senha e criptografia de dispositivo, o armazenamento portátil é fornecido com defesas para prevenir o acesso a dados sensíveis caso o dispositivo seja perdido, roubado ou deixado em uma situação potencialmente vulnerável.

Esta não é uma solução única para todas as necessidades já que técnicas de criptografia variam, e as diferenças mais significativas aparecem ao comparar as soluções de criptografia de hardware e software. Então qual é a melhor? Depende de suas necessidades, mas uma questão mais diligente seria, "Qual é a mais segura?"

A criptografia de software é essencialmente uma escolha de orçamento que vai satisfazer alguns setores com menores operações. Ela também servirá para negócios nos quais as transferências de dados não são consideradas sensíveis e cujas preocupações têm mais a ver com cumprimento das políticas.

Ainda assim, o modus operandi da criptografia de software também é seu calcanhar de Aquiles, já que requer aplicativos voltados ao cliente que confiam em um computador para desempenhar as tarefas de criptografia. Consequentemente, por associação, um dispositivo de armazenamento criptografado de software só é tão seguro quanto o computador host.

A exposição a explorações é algo intensificado já que os hackers com acesso à memória do computador podem "farejar" as chaves de criptografia/descriptografia. Os dados no drive também podem estar sujeitos a ataques de força bruta já que a proteção ao acesso por senha não é necessária se os arquivos criptografados puderem ser acessados e copiados.

Lembre-se, a criptografia com base em software pode precisar de atualizações de softwares de tempos em tempos, o que pode complicar a implementação ao criar um fardo adicional para a equipe de TI. O pior de tudo, a criptografia de software pode ser totalmente removida por funcionários frustrados que têm problemas com a portabilidade de drive nas plataformas. Os usuários de drive podem copiar os dados do drive criptografado para um computador, reformatar o drive para um drive não criptografado e depois copiar novamente os dados para dentro do drive. Neste ponto, os dados não estariam seguros e estariam totalmente vulneráveis à uma violação. Para finalidade de conformidade com as leis e regulamentações sobre privacidade de dados, isto é inaceitável já que a segurança do drive USB pode ser desativada com eficiência.

Criptografia no chip: a solução rápida e difícil

Em contraste, um drive USB criptografado com base em hardware funciona independentemente do computador já que inclui um processador dedicado integrado no drive real que gerencia a criptografia. Isso é um processo de criptografia sempre ligado com proteção contra ataques a senhas por força bruta; dados criptografados não são acessíveis e não podem ser copiados.

Os drives USB criptografados com base em hardware de nível militar e empresarial da Kingston utilizam criptografia AES 256-bit no modo XTS. Como uma técnica de criptografia aprovada no mundo todo, a AES de 256 bits fornece proteções rigorosas aos dados. Utilizando duas chaves separadas em diferentes estágios do processo de criptografia/descriptografia, o modo XTS tem um efeito similar para criptografar os dados duas vezes.

Em uso, a criptografia-chave é derivada do gerador randômico do controlador do drive que desbloqueia a senha do usuário. Já que a autenticação se aplica na criptografia com base em hardware do dispositivo, as chaves de criptografia e outras funções de segurança críticas são protegidas contra explorações comuns como BadUSB, ataques frios de boot, códigos maliciosos e ataques de força bruta.

Um dos benefícios mais imediatos da criptografia com base em hardware é que o desempenho do drive é significativamente melhor do que um drive de software criptografado já que não há descarga de tarefas de criptografia no computador host. Tudo se aplica dentro do drive.

Drives USB criptografados com base em hardware como Kingston IronKey D500S são dispositivos protegidos por senhas que são criptografados prontamente. Em uso, apenas o volume iniciador protegido contra gravação é visível para começar, já que contém o aplicativo usado para autenticar a senha e desbloquear o volume de armazenamento criptografado principal. Este procedimento impede a instalação de qualquer tipo de driver ou software no computador host.

Além disso, os drives USB criptografados com base em hardware da Kingston incluem firmware assinados digitalmente que previnem qualquer manipulação de firmware dentro do dispositivo. Ter esta camada de segurança adicional fornece uma proteção contra ataques como BadUSB que exploram uma vulnerabilidade inerente no firmware do dispositivo USB. Isso pode levar a comandos executados secretamente ou códigos maliciosos serem executados no computador host.

É claro que uma abordagem de 'Bloquear todas as portas limitaria o risco de exploração por BadUSB, mas por quê sacrificar a produtividade com tais práticas ultrapassadas? Como destacado acima, um ambiente seguro pode ser mantido em conjunto com o uso de dispositivos de armazenamento portáteis se simples procedimentos de implementação e aquisição estiverem aplicados para introduzir drives USB criptografados com base em hardware

Trabalho remoto seguro e em conformidade

Para trabalhadores remotos, estar longe das proteções de um ambiente de trabalho seguro de uma empresa exige uma estratégia revisada bem como um novo olhar sobre as prioridades.

Quando se trata de plano de segurança remoto, há algum benefício em bloquear as portas USB do laptop de seu funcionário visando conectá-lo apenas à internet para acessar um servidor para fazer upload ou recuperar documentos? Em movimento, uma conexão de internet aberta tal como um ponto

de acesso Wi-Fi inseguro ou não confiável pode estar disponível e introduzir uma grande variedade de perigos que aumentariam muito a possibilidade de uma violação. Ameaças como vigilância e interceptação de dados através de falsificação, ataques Man-In-the-Middle (MitM) e grampos de rede são apenas alguns dos sofisticados métodos de hacking disponíveis aos criminosos cibernéticos. Mesmo VPNs foram comprometidos.

A conexão de rede à internet de uma organização é apenas outro endpoint e sua exposição inerente faz dela um ponto de entrada alvo e extremamente vulnerável. Abrir o acesso remoto carrega seus próprios riscos de segurança especialmente quando se trata de dados sensíveis.

Confiar drives USB criptografados com base em hardware e protegidos por senha aos trabalhadores remoto elimina efetivamente as potenciais vulnerabilidades de rede. Ainda assim, tais condições exigem uma avaliação mais apurada dos drives USB disponíveis e como eles atendem às exigências de cada ambiente de trabalho remoto. Essa não é uma simples questão de fazer uma escolha sobre a capacidade do drive ou se ele deve ter seu número de série conectado. Isso diz respeito à construção física do dispositivo em si.

Proteções contra manipulação: As opções sólidas

O principal problema aqui é se um drive USB criptografado com base em hardware é à prova de violação ou não. O quão seguro o dispositivo é para tal interferência é refletido em padrões como FIPS 140-3, que possui várias camadas que investigam a resiliência da construção física de um drive sem usar métodos criptografados.

A certificação FIPS-197 relacionada observa apenas os atributos de criptografia com base em hardware e dispositivos tais como SSD Externo Vault Privacy 80 e a série IronKey Vault Privacy 50 que são modelos orientados para empresa onde as exigências de segurança de dados não são de nível militar. Esses drives são menos caros mas são ausentes de proteção contra manipulação do drive físico.

Com a certificação FIPS 140-3 Nível 3 (pendente), os métodos implementados para expor a manipulação do dispositivo são classificados como nível militar. A Kingston fornece esses drives FIPS 140-3 Nível 3 para empresas, governos e militares no mundo todo.

Usar o epóxi internamente para cobrir todo o circuito do drive e colar os componentes internos ao invólucro cria um outro muro de defesa. Qualquer tentativa de abrir a capa de metal seria extremamente difícil e quebraria os chips internos e outros componentes, tirando a funcionalidade do drive. Com esse epóxi duro e opaco aplicado, violar os componentes vitais seria uma tarefa quase impossível. Dispositivos como Kingston IronKey D500S e S1000 contêm esta medida de segurança adicional.

Essas proteções de dispositivos não estão confinadas a medidas físicas somente e o Kingston IronKey S1000 leva a proteção contra violação para outro nível. O cryptochip interno do IronKey S1000 pode detectar qualquer adulteração física e tornará o drive inutilizável assim que o dispositivo for ligado. Confiar em dispositivos de armazenamento USB criptografados com base em hardware para acessar e transferir aquivos sensíveis é um movimento pragmático que facilita as operações remotas sem atrito e garante com eficiência a segurança no campo.

Não deixe de pesquisar as características de segurança e hardware de drives USB para ver se atendem as tarefas de suas necessidades específicas e caso de uso. Cada drive USB deve ser revisado caso a caso com credenciais de confiança ajudando a orientar essas decisões. Qualquer que sejam as prioridades, a Kingston oferece uma gama de opções de customização e soluções para drive USB criptografados com base em hardware com preços acessíveis que atendem todos os tipos de ambientes: de conformidade em geral até as especificações militares mais rígidas.

Segurança em primeiro lugar: Sem redes, sem problemas

Hoje em dia, o escritório não possui mais fronteiras e conforme o trabalho de casa continue aumentando, isso trouxe problemas de vulnerabilidade no acesso remoto à atenção de muitas empresas. Muitos estão vivenciando estes desafios pela primeira vez e estão procurando formas mais seguras de acomodar esta tendência em crescimento.

Para dar suporte a essas necessidades de uma grande variedade de setores, os dispositivos de armazenamento USB criptografados com base em hardware já estão bem estabelecidos e fornecem uma solução segura onde a transferência de dados através de redes pode ser impraticável ou indesejável por diversas razões.

No setor financeiro, reguladores frequentemente solicitam dados para verificar a conduta e conformidade de uma empresa. O risco de exposição é muito maior para ser considerado ao usar uma rede para transferir documentos sensíveis contendo detalhes precisos sobre investimentos, comércio de mercados e outras atividades bancárias confidenciais. A solução simples e eficaz é entregar estas informações em um drive USB criptografado com base em hardware.

O uso de drives USB seguros para transferir arquivos em ambientes de assistência à saúde acontece todos os dias. Também ocorre pela conveniência de médicos e especialistas que desejam analisar arquivos, consultá-los para pesquisa ou apresentar exemplos de caso para estudantes de medicina. Também há muitas necessidades práticas quando se trata de sistemas proprietários como dispositivos médicos de imagem onde o acesso pela rede é ausente ou inseguro. Ao utilizar drives USB criptografados com base em hardware em conformidade, os arquivos podem ser transferidos facilmente para o uso em qualquer outro lugar.

Neste cenário, o Kingston IronKey Keypad 200 (KP200) ganha os holofotes. Como um drive independente de OS, não há volume iniciador para inserir a senha, mas ao invés disso, existe um teclado alfanumérico que desbloqueia o dispositivo para uso em qualquer plataforma. Como um canivete suíço dos drives USB criptografados com base em hardware, seu uso se estende à fabricação; transferência com segurança de aplicativos elaborados por pesquisa de TI e desenvolvimento do mundo das máquinas controlado por plataformas de tecnologia operacional (OT). Para operações de plataformas misturadas que também incluem o Linux, o KP200 é uma das soluções disponíveis mais diretas e seguras.

Os dispositivos de armazenamento USB criptografados com base em hardware desempenham um papel vital também na aplicação da lei. Eles protegem e transferem com segurança arquivos de casos, imagens e outras evidências para os campos operacionais, esquadrões de investigação e equipes forenses. A Kingston oferece um benefício adicional, já que pode fornecer drives com o número de série interno impresso na parte externa da estrutura ao lado do código de barras. Emitir e catalogar drives se torna uma forma simples e fácil de rastrear. É tão fácil quanto inserir manualmente um número de série ou tão rápido quanto escanear um código de barras - a auditoria e a gestão de inventários não poderiam ficar mais fáceis. É uma característica que aparece como padrão nos drives Kingston IronKey D500S, D500SM e S1000B/E mas também está disponível para outros modelos criptografados com base em hardware como parte do programa de customização da Kingston.

O que fazer e o que não fazer

✔ **Usar drives seguros e em conformidade** e revisar as especificações para obter drives que combinem com as necessidades de cada implementação.

✘ **Não autorizar uma política aleatória de Trazer seu próprio dispositivo (Bring Your Own Device, BYOD)** – para qualquer empresa, perder drives não criptografados é um preço muito alto em termos de danos à reputação e financeiros.

✔ **Implementar um pacote de gestão de endpoint** e usar drives USB criptografados com base em hardware que ofereçam características de listas de permissões distintas.

✘ **Não deixar nada ao acaso.** Avalie apropriadamente as exigências de ambientes de trabalho remoto e no local.

✔ **Educar a equipe** sobre as questões de segurança. É do próprio interesse deles que a empresa continue protegida de violações na segurança.

✘ **Não tornar a segurança algo doloroso** para que os usuários procurem alternativas que possam deixar de lado as soluções de TI. Não é por que uma política de cobertura de portas sempre foi aplicada que ela vai se aplicar em todos os cenários. O ambiente de trabalho está mudando e ao escolher as soluções certas, novas políticas podem ser desenvolvidas e aplicadas.

Mobilidade de armazenamento e segurança: De última geração

A proteção por senha, criptografia com base em hardware, proteções contra manipulação, lista de permissões granular, certificado de nível militar FIPS 140-3 nível 3 (pendente) e visão geral de registro são características padrão dos drives USB da Kingston que podem ser implementados sem demora.

Estas sólidas defesas de segurança garantem que o drive USB e seus dados continuem seguros em seu ambiente host. Enquanto as especificações são impressionantes no papel, escolher um modelo aleatoriamente sem qualquer pesquisa não fornecerá necessariamente uma combinação ideal para algumas organizações com exigências mais exatas.

Como um fabricante independente, a Kingston oferece uma ampla gama de opções para satisfazer as necessidades do cliente. Através do programa de customização da Kingston, soluções avançadas estão disponíveis e são projetadas para entregar uma experiência impecável ao usuário.

A customização segura vai além de fornecer à uma organização sua própria PID USB para lista de permissões. O perfil de segurança do aplicativo iniciador também pode ser customizado usando quinze diferentes preferências de detalhes de contato e da empresa para permitir dicas de senha e determinar o número máximo de tentativas de senha. Externamente, a imagem da marca da empresa (co-logo) está disponível bem como uma variedade de cores para drives específicos. Com um pedido mínimo de cinquenta drives, todas essas características fornecem um caminho de integração sem esforço para a implementação de dispositivo.

Se um aplicativo de gestão de endpoint adequado para um armazenamento USB seguro ainda não estiver aplicado, há uma solução de gestão que está disponível para organizações que desejam gerenciar seus drives Kingston incluindo opções para redefinir senhas remotamente.

A onipresença e conveniência do USB tem sobrevivido à uma variedade de tecnologias promissoras e para muitas tarefas o imediatismo e a conveniência do armazenamento USB permanece. Disponível imediatamente e sempre seguros, os drives USB protegidos oferecem uma solução simples que pode ser apreciada prontamente.

Por que se preocupar com violações de dados na rede em ambientes remotos? Com dispositivos de armazenamento USB criptografados com base em hardware Kingston IronKey, a resposta está na palma de sua mão.

Para saber mais sobre como a Kingston pode te ajudar, visite o site kingston.com/ironkey ou para questões mais específicas, pergunte a um dos nossos Especialistas em USB criptografado.

#KingstonIsWithYou #KingstonIronkey

ESTE DOCUMENTO ESTÁ SUJEITO A ALTERAÇÕES SEM PRÉVIO AVISO.
©2023 Kingston Technology CorporationP, 17600 Newhope Street, Fountain Valley, CA 92708 USA.
Todos os direitos reservados. Todas as marcas ou marcas registradas pertencem a seus respectivos proprietários.