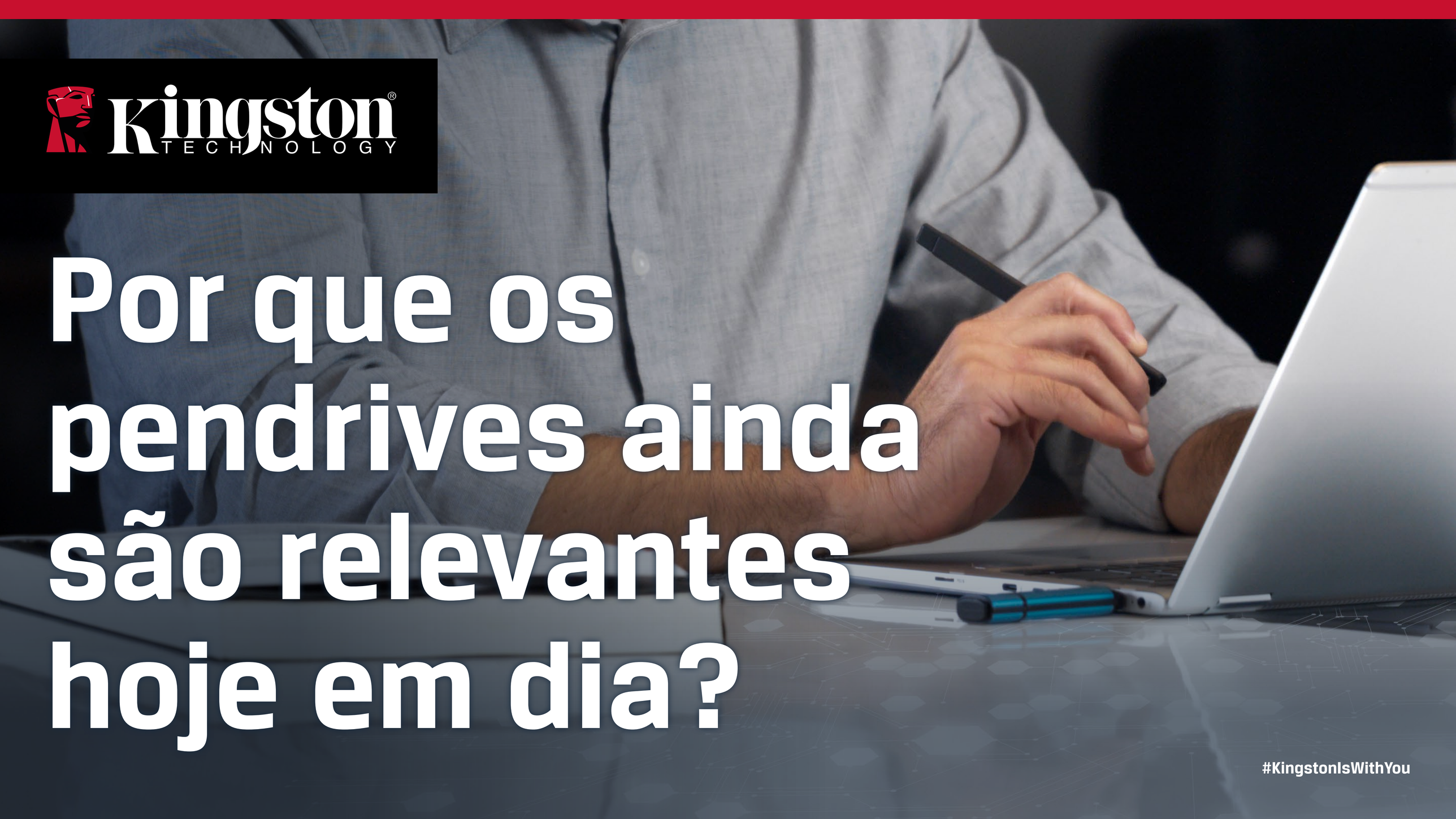

Kingston
TECHNOLOGY
Por que os pendrives ainda são relevantes hoje em dia?
#KingstonIsWithYou

Por que os pendrives ainda são relevantes hoje em dia?

Prefácio e índice

Na atual era digital onde 60% de todos os dados corporativos estão armazenados na nuvem[1], discutir a relevância de uma tecnologia de armazenamento com quase trinta anos de idade pode parecer um pouco estranho. Entretanto, desde seu lançamento, esta opção de armazenamento evoluiu e continua evoluindo.

Faz tempo que os drives USB eram simplesmente uma maneira padrão de conectar arquivos, drives e aplicativos. As soluções de hoje não apenas oferecem velocidades de transferência altamente aprimoradas, mas também oferecem uma mídia portátil segura e confiável obrigatória em várias situações. Mas como os drives USB ainda são relevantes, quando as soluções de armazenamento em nuvem podem facilmente oferecer muitos dos mesmos benefícios?

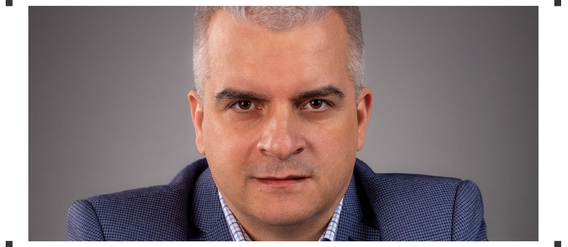
Neste eBook discutiremos onde os pendrives USB se encontram no meio de um cenário dominado pela nuvem. Com o apoio de insights importantes de alguns dos principais especialistas do setor, exploraremos como as organizações atuais estão utilizando os drives USB e debateremos sobre seu lugar no meio da criptografia com base em software, ambientes de armazenamento independentes e segurança de dados de endpoint.

Colaboradores

Esse eBook foi criado com três especialistas no setor de TI e tecnologias emergentes.

Rafael Bloom

Rafael passou sua carreira dentro de cargos seniores de Produtos de Tecnologia, Comunicações de Marketing e Desenvolvimento de Negócios. Sua prática de consultoria se concentra nos novos desafios organizacionais, de produto e de comunicação para mudanças tecnológicas e regulatórias. Esse trabalho altamente diverso envolve uma experiência no assunto sobre conformidade e governança de informação por projeto, privacidade de dados e tecnologias emergentes como AdTech, Telefone Móvel e 5G, IA e Aprendizado de Máquina.



Tomasz Surdyk

Com mais de 24 anos de experiência em segurança de TI dentro de governos, Tomasz é uma figura líder quando se trata de segurança de informações, dados pessoais e segurança cibernética. No passado, ele inspecionou redes e sistemas ICT que processam informações confidenciais e dados pessoais na administração do governo e teve acesso à segurança da OTAN e da UE. Por muitos anos, ele foi proprietário de uma empresa especializada na implementação de soluções de segurança aumentando a segurança de informações comerciais e dados pessoais.

David Clarke

David é reconhecido como um dos 10 principais influenciadores na lista dos 30 pensadores e líderes de pensamento mais influentes nas redes sociais, nas áreas de gestão de risco, compliance e reg-tech do Reino Unido pela Thompson Reuter, além de estar na lista dos 50 principais especialistas globais pela Kingston Technology. No passado, David ocupou várias posições de gestão de segurança como Chefe Global de Serviços de Segurança e Chefe de Infraestrutura de Segurança em empresas FTSE Global 100.

O crescimento do pendrive USB

Quando o primeiro drive de Barramento Serial Universal (USB) apareceu no mercado há mais de 20 anos, sua compatibilidade coletiva foi o divisor de águas no campo da tecnologia de computadores. Com a capacidade de fazer com que múltiplas operações de dispositivo fossem amplamente acessíveis às massas, o USB logo evoluiria, oferecendo transferência de dados significativamente mais rápidas, uma porta USB 3.0 e até capacidades maiores correspondente ao lançamento do primeiro pendrive USB em 2000.

Desde então, a tecnologia seguiu um longo caminho em termos de necessidades de segurança e armazenamento de dados móveis. O foco é sobre os drives USB da geração atual que são projetados com casos de uso muito específicos em mente. De uma perspectiva empresarial, o aumento do trabalho remoto e híbrido, o uso de serviços de nuvem e preocupações com a segurança cibernética estão levando a uma necessidade de soluções mais eficazes. Junto a isso, exigências regulatórias demandam que os dados devem ser armazenados com conformidade. Essas pressões normalmente estão combinadas por sistemas complexos e distribuídos, que podem rodar "no local" e na nuvem.

Depois, há a questão dos crescentes volumes de dados estruturados e não estruturados, como documentos, e-mails, fotos, vídeos e metadados - todos agregando à complexidade das necessidades de armazenamento empresariais em evolução.

Mas se o armazenamento na nuvem pode responder muitos desses desafios, qual a relevância que os drives USB têm no cenário de negócios hoje em dia?

> **Muitas pessoas pensam que drives USB são triviais ou ultrapassados porque seu uso no passado era mais ou menos descartável, de baixo desempenho e baixa segurança. - Rafael Bloom**

Armazenamento portátil que atende à crescente demanda

Embora os padrões mais antigos do uso de drives USB como um meio para armazenamento portátil tenham diminuído, o uso de drives USB de alto desempenho aumentaram para o backup local seguro e pessoal com uma camada extra de proteção de dados e confidencialidade. Isso pode ser muito importante para dados sensíveis em relação à conformidade como registros de RH, dados financeiros, registros de saúde, segurança de propriedade intelectual (IP) e todas as informações pessoalmente identificáveis (PII). Além disso, esta geração de dispositivos conta com rápidas transferências de dados, armazenamento, backup e capacidades de segurança que podem ser usadas para:

- Informações sobre normas regulatórias que precisam ser entregues em mãos
- Documentos financeiros e jurídicos que precisam ser entregues e impressos dentro ou fora do local
- Qualquer ambiente potencialmente hostil onde um ransomware possa ser uma ameaça
- Transferência para sistemas de impressão onde o acesso à rede não é permitido

A Kingston Technology, fornecedora líder de USB criptografados tem acompanhado a crescente demanda com o lançamento de soluções como o Kingston IronKey™ S1000. Este drive USB criptografado é o melhor do tipo e atende aos padrões mais restritos com a capacidade de proteger dados confidenciais ao oferecer a criptografia XTS-AES de 256 bits junto com um criptochip separado que possui fortes proteções contra adulteração. Além disso, tem certificado FIPS 140-2 Nível 3. Isso significa que foi formalmente validado pelo governo dos EUA em relação à eficácia como uma peça de hardware criptográfico, tornando-o ideal para organizações que precisam de paz de espírito adicional quando se trata de proteção de dados.

Tais drives USB criptografados por hardware oferecem soluções de gestão de dispositivo seguras e centralizadas, sejam os dados locais ou em nuvem. O armazenamento de dados criptografados adequados fáceis de usar sem a necessidade do uso de softwares também libera um tempo valioso para o TI, oferecendo soluções projetadas para uma implantação rápida e eficiente.

Armazenamento portátil que atende à crescente demanda

Backup e arquivamento são mais exemplos de onde os drives USB podem ser utilizados para proteger ativos digitais a longo prazo, e independentemente de serviços de nuvem terceirizados. Embora seja verdade que grandes transferências de dados são facilmente realizadas na Nuvem, a PI ainda pode ser sensível o suficiente para valer à pena armazenar em um drive USB criptografado seguro, que pode ser armazenado longe da internet e de forma segura.

E depois, sempre haverá circunstâncias onde uma organização precise que os dados estejam logicamente e fisicamente sob controle, especialmente ao utilizar drives criptografados. E há casos onde o armazenamento em um HDD/SSD não pode ser criptografado. Usar drives USB externos criptografados resolve esse problema, como o Kingston IronKey D300S. Este pendrive USB conta com a criptografia de hardware XTS 256-bit Advanced Encryption Standard (AES), que é um tipo de código de bloqueio que pode criptografar blocos de dados de 128-bit. E quando se trata de criptografar dados além disso, a AES utilizará o modo de código de bloqueio XTS que é capaz de fornecer uma melhor e mais forte proteção de dados do que os modos anteriores.

> Na minha opinião, os pendrives USB ainda são utilizados e são uma parte integral da segurança de dados. Eles são utilizados, dentre outros motivos, para: transferir informações rapidamente entre dispositivos, bem como para sua proteção e armazenamento apropriados.
>
> - Tomasz Surdyk

Criptografia: Com base em hardware X Com base em software

Olhando para como os dados são criptografados, pode-se afirmar que a criptografia de hardware é mais fácil de gerenciar e é mais segura do que a criptografia de software. Isso porque o processo de criptografia é mantido separado do resto do sistema host, dificultando muito sua interceptação ou violação. O gerenciamento centralizado ao nível de dispositivo permite o controle da unidade em relação às conexões de internet e intranet LAN, e pode ser uma excelente ferramenta para:

- Estabelecer e aplicar políticas de uso do USB de grupos e/ou pessoas
- Auditar a atividade dos arquivos para melhor monitoramento conforme eles se movem para dentro e para fora da sua empresa
- Fornecer backup de conteúdo remoto para transporte de dados críticos
- Desabilitar dispositivos remotamente quando um USB for perdido ou estiver comprometido
- Realizar reconfiguração remota da senha quando a mesma for esquecida

Quando drives autorizados são gerenciados corretamente desta forma, o risco dos dados serem copiados e compartilhados é minimizado. Além disso, os drives USB criptografados por hardware do mundo moderno oferecem uma infinidade de recursos de segurança adicionais que ajudam a prevenir que arquivos e mensagens sejam acessadas ou lidas por qualquer pessoa que não seja o destinatário planejado.

> **Eu acredito que a criptografia de hardware é melhor do que a criptografia de software. As diferenças entre os métodos de criptografia de hardware e software são significativas em termos de vulnerabilidades em relação a ataques de força bruta. No caso de dispositivos criptografados por hardware, não é fácil sucumbir a esses ataques. - Tomasz Surdyk**

Criptografia: Com base em hardware X Com base em software

Embora empresas possam considerar a criptografia com base em software por causa do preço, isso pode ser um pouco imediatista. Soluções com base em software compartilham os recursos de criptografia do dispositivo host com outros programas, portanto ele é tão seguro quanto o computador e frequentemente precisa de atualizações de softwares que - se não seguidas - podem deixar você vulnerável. Os drives USB criptografados por software podem estar sujeitos a ilimitados ataques de força bruta para adivinhar a senha, e eles não possuem meios de resistir a ataques de dicionário com base em software - que pode testar milhões de combinações de caracteres em curtos períodos de tempo.

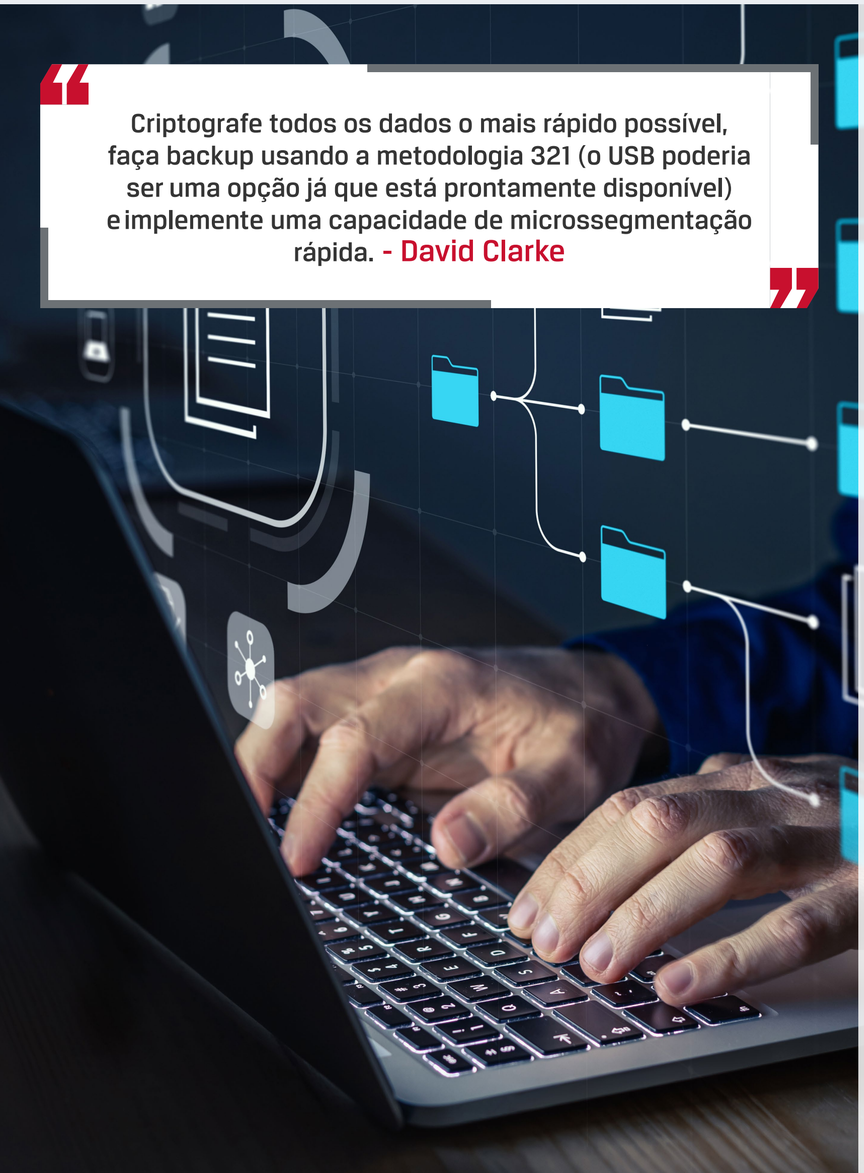
Além disso, a criptografia de software é também uma criptografia removível. Qualquer funcionário com um drive criptografado por software pode copiar os dados para fora, formatar o drive USB e a criptografia é removida. Pode-se então copiar de volta os arquivos de dados e utilizar o drive sem o incômodo da autenticação em diferentes plataformas e sistemas operacionais.

Como mencionamos anteriormente, com a criptografia com base em hardware, a "criptografia" física - e subsequente armazenamento de dados - ocorre independentemente do sistema host. Isso garante uma camada extra de defesa, se os sistemas já foram comprometidos.

Isso não pode ser negligenciado, particularmente para setores como o de finanças, saúde e governo. Isso porque regulações como a Health Insurance Portability and Accountability Act (HIPAA) e o Payment Card Industry Data Security Standard (PCI DSS) frequentemente possuem exigências restritas em relação à criptografia de informações sensíveis.

Estar em conformidade com esses regulamentos utilizando dispositivos criptografados por hardware ajudará as organizações a evitarem grandes multas, processos judiciais e danos potencialmente devastadores à reputação. Embora os drives criptografados por hardware possam ser mais caros do que drives USB mais baratos, os custos judiciais de uma violação podem facilmente pagar centenas de drives em apenas algumas horas de taxas de consultoria jurídica.

A crescente necessidade de proteger dados sensíveis



> Criptografe todos os dados o mais rápido possível, faça backup usando a metodologia 321 (o USB poderia ser uma opção já que está prontamente disponível) e implemente uma capacidade de microssegmentação rápida. - David Clarke

Quando se trata de proteger dados sensíveis contra perda ou roubo, todas as organizações têm a obrigação de garantir que seus dispositivos tenham recursos de segurança adequados. Também é importante considerar que embora haja uma variedade de ameaças cibernéticas em evolução, o nível de maturidade digital e as habilidades de gestão de dados de endpoint próprias dos usuários permanecem um proeminente fator de risco se não tratados. Ameaças internas que incluem perda de controle de dados ou dispositivos de armazenamento USB, a transmissão de dados fora de um ambiente seguro, o uso de drives USB não criptografados e o compartilhamento de senhas podem resultar na falta de diligência prévia do usuário final. Tudo isso pode ser evitado com treinamento adequado, educação e as soluções de drive USB corretas.

> As organizações devem ter um mapa claro de seus dados, incluindo o nível de importância e/ou sensibilidade de todos os seus conjuntos de dados, com o plano tratando primeiro dos dados mais importantes, seja removendo fisicamente a conexão aos dados ou escurecendo a fonte de dados. Poder isolar sistemas afetados rapidamente é primordial - e mais uma vez, ter um plano documentado que você tenha praticado é vital. - Rafael Bloom

O pré-planejamento e uma estrutura de comunicação bem praticada também desempenham um papel fundamental ao lidar com uma potencial ameaça. As ameaças cibernéticas de hoje têm o objetivo de atingir os pontos fracos das organizações.

O melhor momento para desenvolver um plano de USB criptografado é antes de precisar de um, incorporando políticas e drives USB na estratégia geral de segurança de sua empresa. Não ter nenhum plano aplicado para USBs criptografados e nenhuma diretriz faz com que você não tenha nada para desenvolver, e sua organização fica aberta ao risco em todos os níveis - incluindo não estar em conformidade com as regulamentações, como a Data Protection Regulation (GDPR), no artigo 32 declarando especificamente que os dados sensíveis devem ser criptografados.

> Dados sensíveis do usuários. Perder isso aumenta a responsabilidade e afeta significativamente a imagem e a segurança da empresa. Visando proteger os dados sensíveis, várias soluções de segurança devem ser utilizadas, incluindo a criptografia de dados. - Tomasz Surdyk

Proteção de dados financeiros sensíveis

Junto às implicações de segurança, também há normas de conformidade às quais o armazenamento de dados e soluções de backup devem aderir. Algumas dessas práticas, como a necessidade de gerenciar e aplicar programações de retenção de dados, são comuns em verticais, enquanto outras, como migração de dados empresariais para a nuvem, são tratados de forma muito diferente.

Em muitos verticais, como serviços financeiros, regulamentações entraram em vigor e o gerenciamento apropriado de dados se tornou obrigatório. Os bancos inicialmente ficaram reticentes em usar terceiros para armazenamento e backup, e muitos ainda insistem em ter a propriedade de toda a sua infraestrutura de dados.

Instituições financeiras também são obrigadas a estar em conformidade com uma crescente lista de normas e regulamentos de segurança de dados, como a Sarbanes-Oxley Act (SOX) e a General Data Protection Regulation (GDPR). Entretanto, conforme aumenta o número de funcionários e contratados móveis, aumenta também o risco de vazamento de dados e falha na conformidade com os mandatos impostos por tais leis e normas.

A verdade é que os esforços de conformidade podem ser comprometidos de forma surpreendentemente fácil se os funcionários móveis não protegerem suas identidades digitais, espaços de trabalho portáteis, registros de clientes e dados financeiros que carregam. É por isso que mais organizações estão mudando para soluções de segurança móveis como os drives USB criptografados Kingston IronKey, para proteger aplicativos e identidades digitais não importando onde seus funcionários estejam.

> **Quando você considera a tendência geral de mudança para uma pegada de TI mais distribuída e a absoluta escalabilidade da infraestrutura de Nuvem, é fácil ver como a maioria dos setores e o volume de SMEs não estão mais se preocupando em administrar salas de servidor refrigeradas. - Rafael Bloom**

Acesso seguro aos dados de saúde de pacientes

A saúde é outro setor onde a segurança de dados é mais importante do que nunca. As informações do paciente estão sob um risco ainda maior de serem roubadas, com violações expondo 45,67 milhões de registros de pacientes em 2021, o maior valor anual desde 2015[2]. Quando se trata de backup e armazenamento de dados, os dados do paciente são informações médicas abrangentes e críticas que permitem que os provedores de saúde tratem seus pacientes de forma segura.

Podem incluir tudo desde arquivos de Registro de Saúde Eletrônico (EHR) contendo históricos de saúde, testes, fotografias e imagens de radiografias, até arquivos administrativos incluindo registros de pagamento, seguro do paciente e contas a pagar. Com uma crescente força de trabalho móvel e um mercado de saúde global que está sofrendo grandes perturbações e transformações, é de se esperar que os provedores de saúde hoje em dia estejam preocupados com a segurança de dados.

> **Com o ransomware em particular sendo um tipo de setor em crescimento, toda organização que lida com dados sensíveis deve considerar como operar sob extrema pressão. - Rafael Bloom**

E além disso, não antecipar riscos e não atender mandatos restritos como a Health Insurance Portability and Accountability Act (HIPAA) ou a Health Information Technology for Economic and Clinical Health Act (HITECH) pode resultar em uma violação de dados de saúde custosa, o que pode futuramente abalar a confiança do paciente, parceiro ou regulador.

Com soluções como a variedade de drives USB criptografados Kingston IronKey, as organizações de saúde podem definir políticas para senhas, uso de aplicativos, recuperação e mais - em vários drives ou milhares deles, de um único console. Trabalhadores móveis e de linha de frente podem ser empoderados para auxiliar mais pacientes, com soluções amigáveis para o usuário que acabam com a necessidade dos funcionários instalarem drivers ou outro software, visando acessar seus dados armazenados com segurança. Enquanto usuários e administradores podem bloquear dados de forma rápida e fácil, não importa onde estejam.

O drive USB em um futuro de armazenamento em nuvem

> O armazenamento de dados na Nuvem é o presente e o futuro. Eu ainda defendo que os dados seguros fisicamente, por ex., utilizando drives USB criptografados, são a forma mais segura. Os usuários não possuem controle total sobre o que acontece na nuvem. Entretanto, temos o controle sobre os dados em drives USB criptografados, que nós mesmos protegemos e armazenamos. Além de nós, ninguém tem acesso a essas mídias. - Tomasz Surdyk

Agora que os benefícios dos drives USB estão claros, qual é exatamente seu papel em um futuro de armazenamento em nuvem?

Há uma década, os drives USB estavam em alta demanda sendo a ferramenta principal para armazenar e transferir dados de forma conveniente. Entretanto, com o impacto de novos modelos de trabalho híbrido e equipes cada vez mais distribuídas, a nuvem agora fornece acesso simples e rápido de vários dispositivos às informações armazenadas. Enquanto pendrives eram imensamente populares devido ao conforto exclusivo que ofereciam ao transportar arquivos. Hoje em dia, serviços de armazenamento em nuvem oferecem maior facilidade de portabilidade de arquivos.

Dito isso, ainda há muitas limitações quando se trata de armazenamento em nuvem. É preciso conectividade de rede, que não apenas dita como e quando os arquivos podem ser guardados ou transferidos - isso adiciona uma preocupação extra de segurança. Quando uma empresa autoriza o uso da nuvem, não é necessariamente possível controlar de onde os dados são acessados. Portanto, o simples ato de acessar um VPN usando uma conexão Wi-Fi particular ou pública abre para o risco de ser hackeado. Além disso, serviços de Nuvem são muito atraentes para agentes de ameaças, com a maioria de todos os malwares (61%) agora enviados através de aplicativos de nuvem[3].

> É interessante considerar o que acontece quando a nuvem está indisponível, os cenários onde os dados devem estar 100% disponíveis e onde o armazenamento a longo prazo poderia criar uma vulnerabilidade. - David Clarke

O drive USB em um futuro de armazenamento em nuvem

A criptografia USB, por outro lado, pode ser feita através do hardware do dispositivo ou através de software. Criptografia sem software centrada em hardware é a maneira mais eficiente para fornecer proteção contra ataques cibernéticos. É uma solução excelente e simples para se proteger contra violações de dados e pode estar em conformidade com normas rígidas com a mais nova segurança em proteção de dados, visando ajudar as organizações a gerenciarem ameaças de forma confidencial e reduzir os riscos.

Como são drives USB criptografados por hardware e integrados, não precisam de um elemento de software no computador host. Nenhuma vulnerabilidade de software também elimina a possibilidade de força bruta, sniffing e ataques hash de memória. Drives USB criptografados por software também enfrentam o risco de qualquer usuário poder desabilitar a criptografia formatando o drive em qualquer computador e utilizar o drive para armazenar dados sensíveis de uma forma inapropriada.

Os drives USB criptografados por hardware também oferecem uma maneira física excepcional de manter os dados em segurança. Eles permitem que critérios de acesso de informações sejam aplicados por um usuário ou administrador, e podem integrar-se com soluções de endpoint local existentes. Isso faz com que eles se tornem uma solução conveniente e com bom custo-benefício para muitos cenários onde o armazenamento em nuvem não funcionaria, ou não seria uma solução eficiente. Pode ser quando os dados precisem ser armazenados de dispositivos que não estejam em rede, que precisem ser privados ou necessitem de acesso quando off-line.

> **Se pensarmos sobre dados sendo 'quentes' ou 'frios' dependendo de seu nível de utilidade em uma base diária para uma organização, então pode ser mais eficiente colocar dados 'frios' na nuvem e utilizar mais o armazenamento USB localizado para dados 'quentes', se a continuidade operacional e alto desempenho forem mais importantes para a organização, ou para um processo ou função particularmente crítica para os negócios. - Rafael Bloom**

Resumo

Como não podemos prever a chegada de inovações futuras, o que podemos oferecer é um premiado portfólio de drives USB, oferecendo uma variedade dinâmica de soluções criptografadas para todos os níveis de exigência de proteção de dados móveis. Desde drives USB que contam com teclado alfanumérico para uma proteção por PIN fácil de usar; certificado FIPS 140-2-Nível 3 para o mais alto nível de criptografia junto a proteções contra adulteração; até a tecnologia SuperSpeed USB 3.1 que não compromete a segurança, os produtos Kingston IronKey são projetados para atender seus desafios de dados, com drives USB que prometem transporte de dados e soluções de armazenamento de dados móveis poderosos e eficientes.

Nossa equipe especializada está pronta para te auxiliar em cada etapa de sua jornada de armazenamento de dados, oferecendo confiança quando se trata de te ajudar a encontrar a solução de armazenamento certa para atender suas necessidades.

Temos habilidades e capacidades técnicas para te ajudar a manter suas informações confidenciais seguras e em conformidade com os novos regulamentos, seja querendo desenvolver um plano de USB criptografado, identificar os melhores drives USB para seus negócios ou estabelecer e aplicar políticas de segurança. Oferecendo um serviço altamente personalizado, estamos comprometidos com a entrega de produtos que auxiliam em suas prioridades de armazenamento de dados, permitindo que você mantenha o ritmo a uma velocidade sem precedente na qual o mundo dos negócios está se movendo.

Sobre a Kingston

Com 35 anos de experiência, a Kingston possui o conhecimento para identificar e resolver seus desafios de dados móveis - fazendo com que sua força de trabalho opere com segurança sem comprometer sua organização.

1. Statista - https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data
2. SC Magazine - https://www.scmagazine.com/analysis/breach/breaches-exposed-45-67m-patient-records-in-2021-largest-annual-total-since-2015
3. Infosecurity Magazine - https://www.infosecurity-magazine.com/blogs/cloud-services-top-of-mind-phishers

#KingstonIsWithYou