



Segurança de Endpoint Otimizada Explicada e Explorada em Parceria com a Matrix42

MATRIX42

#KingstonIsWithYou



Segurança de Endpoint Otimizada Explicada e Explorada em Parceria com a Matrix42



Introdução

A proteção de dados é uma preocupação fundamental para empresas, governos e indivíduos no mundo de hoje.

Violações de dados, hacking e o elemento humano são lembretes constantes de ameaças e riscos em todo o mundo. Tanto os custos monetários quanto os custos à reputação vinculados a uma violação de dados podem ser astronômicos. As exigências de segurança cibernética avançada e as estratégias DLP Endpoint para proteção contra perda de dados dependem de armazenamento e memória confiáveis e eficientes.

O uso de criptografia, armazenamento rápido e memória combinados com as melhores práticas, padrões e políticas representam um grande passo. Laptops e pendrives perdidos deixam tanto indivíduos quanto empresas vulneráveis à exposição de informações pessoais e privadas. A Kingston oferece soluções de prevenção às ameaças para ajudar a minimizar os riscos e, ao mesmo tempo, complementar um plano de segurança existente ou em desenvolvimento.



Conteúdo

Este pequeno eBook vai examinar soluções de endpoint e onde os pendrives criptografados da Kingston, seu programa de personalização e o software de proteção de dados EgoSecure da Matrix42 ajudaram a resolver seis diferentes desafios de setores da indústria e lhes forneceram uma solução que atendia suas necessidades de negócios.

Nós nos aprofundaremos nesses seis setores e veremos como eles enfrentam seus desafios de segurança de endpoint.

Índice

Seção 1	Caso de uso da indústria – Setor público	4
Seção 2	Caso de uso da indústria – Setor de Saúde	5
Seção 3	Caso de uso da indústria – Finanças	6
Seção 4	Caso de uso da indústria – Automotivo	7
Seção 5	Caso de uso da indústria – Telecomunicações	8
Seção 6	Caso de uso da indústria – Produção	9
Seção 7	Soluções Kingston e Matrix42	10
	Resumo	11
	Sobre a Kingston	12



Seção 1: Caso de uso da indústria

Setor público



Situação:

Dentro do setor público, o uso de pendrives é muito comum. Por exemplo, as secretarias de ordem pública devem copiar as fotos tiradas associadas a infratores de estacionamento e infrações administrativas de câmeras digitais para os sistemas das autoridades via cabo USB. As autoridades policiais recebem dados de investigações em dispositivos externos para armazenamento de dados. Os dados precisam ser regravados e deve ser evitado o acesso não autorizado.

Desafio:

Devido à grande demanda de dispositivos USB, os funcionários solicitam unidades USB regularmente. O uso de dispositivos de armazenamento privados e não autorizados deve ser impedido por razões de segurança. Se um funcionário precisar de um novo dispositivo de armazenamento USB, ele deve ser disponibilizado tão rápido quanto possível através do suporte técnico para que os funcionários não sejam perturbados em seu trabalho. É importante observar que não surge nenhum problema de segurança pelo uso dos dispositivos USB apropriados.

Solução:

Combinando controle do dispositivo, filtro de dados e criptografia, o seguinte cenário pode se tornar possível:

Dispositivos desconhecidos são geralmente bloqueados nos endpoints de computadores. Dispositivos de armazenamento de dados, como câmeras digitais, somente são permitidos para certas funções como a leitura de arquivos de imagem. Operações de gravação geralmente são criptografadas e somente são permitidas em dispositivos USB autorizados. Todos os acessos de dados são registrados. O gerenciamento de dispositivos autorizados pode ser simplificado personalizando-se números de série e IDs de hardware. Assim, o Gerenciamento de Serviços Matrix42 permite ao usuário solicitar o pendrive personalizado da Kingston Technology no Portal de Autosserviço. Após um processo de aprovação, o dispositivo USB é automaticamente autorizado para uso no EgoSecure Data Protection.

“ Nossos funcionários estão animados com o fato de novos dispositivos USB serem fornecidos de forma fácil e rápida após o breve processo de aprovação. Estamos muito felizes com o programa de customização da Kingston Technology e a fácil administração da combinação de gerenciamento de serviços e segurança de endpoint da Matrix42. ”

Chefe de suporte técnico, Setor público

Seção 2: Caso de uso da indústria Setor de Saúde



Situação:

Dispositivos de armazenamento externos continuam a ser frequentemente usados como meio de transferência de dados de/para funcionários ou outras instituições.

Por exemplo, hospitais na Alemanha devem fornecer o Registro de Câncer com informações sobre casos atuais de câncer e seu desenvolvimento. Para maior facilidade, esses dados são frequentemente transferidos por dispositivos móveis de armazenamento de dados.

Médicos também gostam de levar documentos, como dados de pesquisa, para suas respectivas palestras em unidades USB.

Desafio:

Dados de pacientes são altamente reservados e não devem cair nas mãos de pessoas não autorizadas. Para tanto, a proteção de dados deve ser ampliada e fortalecida. Se um pendrive for perdido, isso pode se tornar um grande problema, não apenas devido ao GDPR, mas para o bem-estar dos pacientes. Por essa razão, é importante que o acesso ao armazenamento USB de dados seja controlado, monitorado e criptografado.

Solução:

A EgoSecure Data Protection combina várias medidas de proteção como controle de acesso, auditoria de dados, filtro e criptografia em uma única solução. Os administradores de TI podem decidir a quais funcionários será concedido acesso a quais dispositivos. Podem ser feitas exceções, por exemplo, por número de série e ID do hardware. Esses identificadores podem ser definidos graças ao programa de customização da Kingston Technology, para que apenas um valor precise ser configurado no gerenciamento do EgoSecure Data Protection para permitir que sejam usados somente dispositivos aprovados pela empresa. Isso minimiza enormemente o esforço da administração e aumenta a segurança dos dados (GDPR, CCPA, HIPAA etc), pois o acesso é criptografado e monitorado.

“ Nós já usamos pendrives criptografados da Kingston. Agora, com o EgoSecure Data Protection, também podemos assegurar que o rastreamento das transferências de dados dos pacientes é realizado de acordo com o EU-GDPR. ”

CISO, Hospital Universitário



Seção 3: Caso de uso da indústria Finanças



Situação:

Os bancos estão sujeitos a várias exigências de conformidade. Uma dessas exigências é a conformidade com o padrão PCI-DSS (Payment Card Industry Data Security Standard - Padrão de Segurança de Dados do Setor de Cartões de Pagamento). As exigências de PCI-DSS incluem a necessidade de criptografia de dados, análise de vulnerabilidade e filtragem de dados. O objetivo é minimizar ou impedir totalmente ameaças e riscos de segurança de TI.

Desafio:

Há muitos riscos relacionados à segurança de TI existentes no endpoint. Funcionários precisam trabalhar com informações de cartões de pagamento de consumidores e empresas e processar dados confidenciais de instituições financeiras diariamente e são expostos, portanto, à ameaça de dados na nuvem, e-mail, USB e da Internet estarem comprometidos por malware, ou dados poderiam acidentalmente cair nas mãos de terceiros se não forem adequadamente protegidos. Um incidente desse tipo poderia ser um risco com implicações financeiras para um banco em termos de GDPR, PCI-DSS, mas também quanto a lei Sarbanes-Oxley. Além disso, criminosos cibernéticos tentam influenciar ou manipular sistemas bancários de várias maneiras e estão se tornando mais criativos nesse

processo. Mais recentemente, por exemplo, houve um crime cibernético relacionado a caixas eletrônicas onde o fornecimento de energia foi interrompido e o sistema foi iniciado com um dispositivo USB inicializável para roubar o dinheiro.

Solução:

Os sistemas de TI devem estar seguros por medidas de proteção de muitas camadas. Isso pode ser conseguido através do controle do aplicativo, controle do dispositivo, detecção de anomalias, UEBA (User and Entity Behaviour Analytics - Analítica da Conduta de Usuário e Entidade), monitoramento e criptografia total do disco com PreBoot Authentication. O Matrix42 pode implementar tudo isso em um ecossistema integral e automatizado, de modo que apenas aplicativos autorizados e dispositivos USB criptografados sejam permitidos. Além disso, atividades suspeitas ou maliciosas são detectadas e mais medidas são iniciadas automaticamente. Em relação ao uso de unidades USB, a combinação de unidades USB customizadas da Kingston Technology ajuda a garantir que dispositivos sejam incluídos na lista de permitidos com facilidade e que os dados sejam criptografados e possam ser rastreados. Isso aumenta enormemente a conformidade sem esforço adicional.



“ Com a Proteção de Dados EgoSecure e a funcionalidade de inclusão na lista de permissões, somente permitimos que unidades USB criptografadas sejam aprovadas. Nós incluímos na lista de permissões unidades USB criptografadas da Kingston com ID de hardware personalizado - outros dispositivos não são permitidos. Isso reduz o esforço administrativo - e aumenta a segurança! ”

Gerente de TI, Empresa Financeira

Seção 4: Caso de uso da indústria Automotivo



Situação:

No setor automotivo, o uso de dispositivos USB está presente em várias áreas. Por exemplo, dados de pesquisa são armazenados em dispositivos de armazenamento externo e distribuídos entre os respectivos engenheiros da empresa. Para configurar máquinas de produção, os arquivos são transportados de ambientes de TI para ambientes de TO (Tecnologia Operacional). Todos esses dados são altamente reservados e devem ser protegidos contra espionagem industrial e roubo de dados, de outra forma o know-how construído poderia cair em mãos erradas.

Desafio:

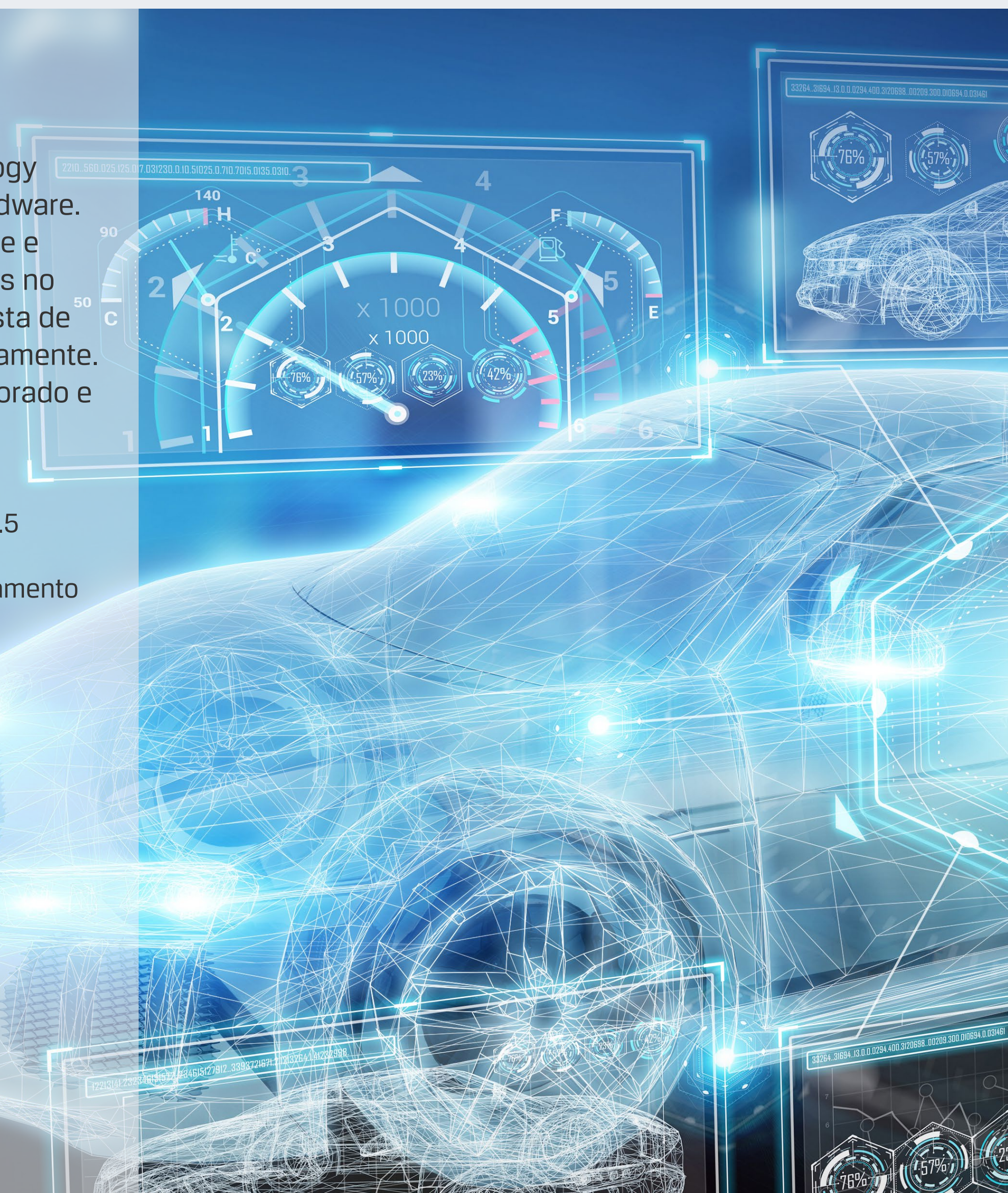
O setor automotivo está sujeito a exigências de conformidade como TISAX, proteção de protótipos, ENX, ISO27001, "conexão com terceiros" e GDPR. Na TISAX (Compartilhamento confiável de avaliação de segurança da informação), os artigos de Controle 9.1, 9.5 e 10.1 dispõem que os acessos a dados devem ser controlados, monitorados, filtrados e criptografados. Essas medidas também devem ser observadas nas outras exigências de conformidade, como a GDPR e ISO27001 em todas as áreas das empresas automotivas.

Solução:

As unidades USB criptografadas da Kingston Technology protegem os dados com criptografia baseada em hardware. Esses dispositivos podem receber um número de série e ID de hardware personalizados, que podem ser usados no EgoSecure Data Protection para serem incluídos na lista de permissões para uso específico de dados, automaticamente. E além disso, o movimento dos dados pode ser monitorado e analisado se houver qualquer atividade suspeita.

“ Com a Matrix42 e a Kingston Technology, foi possível implementar as exigências de TISAX como o Controle 9.5 (acesso às informações e aplicativos) e Controle 10.1 (criptografia) sem mudanças importantes no comportamento do usuário. ”

CTO, fornecedor automotivo



Seção 5: Caso de uso da indústria Telecomunicações



Situação:

Prestadores de serviços de telecomunicação têm muitas informações sobre os clientes. Essas informações são altamente reservadas, especialmente em relação a GDPR. Portanto, precisam ser tomadas medidas suficientes para evitar perda de dados e roubo de dados.

Desafio:

Funcionários de empresas de telecomunicação trabalham com dados de clientes todos os dias. A maior parte dos dados é armazenada dentro de aplicativos empresariais. Entretanto, há o risco de que os contratos de clientes ou até as exportações de banco de dados sejam armazenadas em endpoints e em dispositivos externos à eles. Para troca de dados os usuários frequentemente usam armazenamento externo. Assim é muito importante que práticas de armazenamento de dados incorretas sejam detectadas e corrigidas ou protegidas.

Solução:

Para simplificar o processo de aquisição, a Kingston Technology criptografou unidades USB com IDs personalizadas do produto que podem ser rapidamente adquiridas através de uma lista de permissões predefinidas no EgoSecure Data Protection e entregues através

do Catálogo de Serviço Matrix42. O armazenamento e exportação de dados, que podem conter informações confidenciais, podem ser automaticamente identificadas e reparadas por uma inspeção profunda dos dados com base em escaneamento de "dados em uso" e "dados inativos". O movimento dos dados é registrado centralmente. Assim, o funcionário pode receber o novo equipamento para armazenamento de dados logo após este ter sido requisitado e aprovado. Isso pode garantir que ele estará em conformidade com o GDPR.

“ Graças ao portal de autosserviço Matrix42, nossos usuários podem requisitar a mídia de armazenamento que precisam. Depois que o pedido for aprovado e entregue, o dispositivo será autorizado pelo controle de dispositivos do EgoSecure. A combinação da Matrix42 com a Kingston Technology aumenta a produtividade e a segurança em nossa empresa. ”

**CTO, Prestador de Serviços
de Telecomunicações**



Seção 6: Caso de uso da indústria Setor de Produção



Situação:

O ouro do futuro são os dados digitais. Esses dados valiosos nos setores de produção incluem planos de produção, dados sobre clientes e fornecedores e know-how da empresa. Se esses dados forem perdidos, pode ocasionar não apenas penalidades graves do ponto de vista do GDPR, mas também problemas exponenciais e à reputação. Infelizmente, USBs são encontrados em táxis, lavanderias, aeroportos, estações de trem ou estacionamentos, todos os dias.

Desafio:

Dispositivos de armazenamento frequentemente contêm dados altamente confidenciais e, infelizmente, esses dados não estão criptografados. Há também o risco de técnicos de suporte usarem transportadores externos de dados para instalar atualizações em máquinas de produção. Esses dispositivos externos trazem o risco de introduzir malware na rede.

Solução:

As unidades USB criptografadas da Kingston Technology protegem os dados com criptografia baseada em hardware. Esses dispositivos podem ser entregues com um número de série e ID de hardware personalizados, que podem ser usados no EgoSecure Data Protection para serem incluídos na lista de permissões para uso específico de dados, automaticamente. E além disso, o movimento dos dados pode ser monitorado e analisado se houver qualquer atividade suspeita.

“ A criptografia dos nossos dados de produção é muito importante para nos proteger contra roubo de dados. Esses dados altamente confidenciais somente são permitidos em unidades USB criptografadas da Kingston aprovadas através do filtro de arquivos do EgoSecure Data Protection. Em todos os outros dispositivos USB, os dados de produção são bloqueados e o acesso à gravação em armazenamentos de dados externos é protegido simultaneamente. ”

Diretor de Segurança de TI, Setor de Produção





Seção 7: Soluções Kingston Technology e Matrix42



O uso de criptografia, armazenamento rápido e memória combinado com as melhores práticas, padrões e políticas representam um grande passo. Laptops e pendrives perdidos deixam tanto indivíduos quanto empresas vulneráveis à exposição de informações pessoais e privadas. A Kingston Technology oferece soluções de prevenção às ameaças para ajudar a minimizar os riscos e, ao mesmo tempo, complementar um plano de segurança existente ou em desenvolvimento.

Unidades USB Criptografadas Kingston Technology

As unidades USB com criptografia baseada em hardware da Kingston Technology apresentam soluções de proteção de dados móveis dentro e fora do firewall de uma organização. Projetados para proteger dados que requerem segurança máxima, essas unidades ajudam a atender padrões, diretivas e regulamentos específicos do setor. Os produtos estão em conformidade com a TAA, certificados FIPS e estão disponíveis em capacidades de até 128GB, tornando-os ideais tanto para usuários corporativos quanto para órgãos do governo.



Programa de Personalização de Segurança

Você pode personalizar as unidades USB criptografadas da Kingston Technology de diversas maneiras para atender as necessidades da sua empresa. Adicione recursos selecionados para criar unidades exclusivas e indispensáveis. A Kingston Technology oferece formas fáceis e práticas de fazer o pedido da sua unidade USB criptografada personalizada através do seu revendedor preferido. A linha de produtos USB criptografados da Kingston Technology inclui as séries DTVP30, DT4000G2 e IKD300S. Esse programa oferece as opções solicitadas mais frequentemente pelos clientes, incluindo numeração em série, senha dupla e logo personalizados. Com um pedido mínimo de 50 peças e quantidade de repetição de 25 peças, o programa oferece com precisão o que sua empresa precisa.

Matrix42 EgoSecure Data Protection

O Matrix42 EgoSecure Data Protection oferece às empresas gerenciamento de segurança de 360° para a prevenção e proteção dos dispositivos, sistemas e dados. A solução automatiza todo o processo desde a prevenção e detecção até as contramedidas no evento de danos, sem perda de produtividade.

A proteção de dados e a segurança cibernética podem parecer uma responsabilidade assustadora. As exigências no trabalho digital mudaram significativamente com os funcionários tendo a capacidade de decidir por eles mesmos quando, onde e com qual dispositivos irão trabalhar. A combinação certa de unidades USB criptografadas com base em hardware e gerenciamento de endpoint por software pode ajudar as organizações a obter o controle dos dispositivos da sua empresa. E portanto, mitigar o risco de violações de dados e apoiar sua atual estratégia de conformidade com o GDPR.





Sobre a Kingston

Com mais de 30 anos de experiência, a Kingston Technology possui o conhecimento para identificar e resolver seus desafios de segurança de endpoint sem comprometer sua empresa.

©2021 Kingston Technology Corporation, 17600 Newhope Street, Fountain Valley, CA 92708 USA. All rights reserved.
Todos os direitos reservados. Todas as marcas ou marcas registradas pertencem a seus respectivos proprietários.

#KingstonIsWithYou