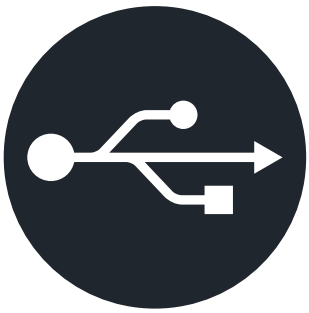
Cara mengizinkan akses drive USB

tanpa membahayakan keamanan titik akhir

#KingstonIsWithYou #KingstonIronkey

Pendahuluan

Spesifikasi resmi USB 1.0 yang dirilis pada Januari 1996 menandai era baru keseragaman, kemudahan, dan keserbagunaan bagi para vendor perangkat periferal dan pengguna akhir. Pada 27 tahun berikutnya, USB tetap menjaga kompatibilitas mundur pada setiap revisinya dan bertahan sebagai landasan antarmuka perangkat keras komputer, mulai dari server hingga smartphone.



Kesederhanaan plug-and-play dan kecepatan USB yang terus meningkat menjadikan penyimpanan portabel USB berkembang sebagai salah satu teknologi yang paling unggul. Akan tetapi, kemudahan tersebut memiliki konsekuensi dalam hal keamanan data. Dewasa ini, tanpa penggunaan peralatan yang tepat seperti perlindungan titik akhir di komputer host dan praktik keamanan data yang tepat, para pengguna dengan sikap ceroboh ketika menggunakan penyimpanan USB portabel dapat mengekspos diri mereka sendiri dan orang lain terhadap kemungkinan pembobolan data yang dapat merugikan dirinya dan bahkan membahayakan keseluruhan organisasi atau badan pemerintah.

Selain perlindungan lingkungan host, drive USB juga harus diamankan dengan perlindungan kata sandi dan enkripsi perangkat keras pada perangkatnya. Langkah ini memberikan pertahanan paling kuat terhadap intrusi. Kami akan membahas beberapa praktik terbaik dalam penggunaan drive USB yang lebih aman sekaligus pengamatan lebih mendalam tentang drive USB secara umum.

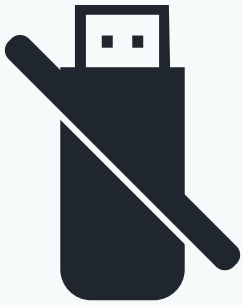
Meskipun pendekatan gabungan adalah hal ideal, tetapi hal yang paling penting adalah ketangguhan enkripsi dan komponen perangkat keras dari drive USB itu sendiri. Ketangguhan enkripsi dan komponen memberikan manfaat terhadap berbagai sektor, mulai dari keuangan, perawatan kesehatan hingga manufaktur dan militer. Ketangguhan enkripsi dan komponen juga berperan dalam pekerjaan jarak jauh ketika akses jaringan mungkin tidak tersedia, mengalami kerentanan, atau tidak praktis.

Drive USB terenkripsi perangkat keras tersedia dalam berbagai peringkat sertifikasi dengan menyediakan beragam fitur keamanan. Dengan mengevaluasi atribut dan peluang kustomisasi pada drive terenkripsi perangkat keras, kesesuaiannya sebagai solusi mandiri juga terlihat pada keunggulan reputasinya pada semua jenis lingkungan yang sensitif.

Otoritas port: Penyimpanan USB bertemu dengan Perangkat lunak pencegahan kehilangan data dan manajemen titik akhir

Selama beberapa dekade, aplikasi antivirus dan anti-malware telah menawarkan perlindungan di tingkat paling mendasar – memindai otomatis unduhan dan perangkat yang ditambahkan serta melaporkan atau bertindak atas konten yang mencurigakan. Perlindungan dari perangkat lunak Next Generation Anti-Virus (NGAV) melakukan hal ini dengan lebih baik. Alih-alih hanya mengandalkan database antivirus yang terus-menerus diperbarui, NGAV menambahkan fitur pembelajaran mesin dan deteksi perilaku yang dapat mengidentifikasi dan mengurangi ancaman yang belum dikenal.

Fitur tersebut bukan satu-satunya kemampuan yang dimilikinya. Bagi pengguna yang menginginkan perlindungan lebih kuat terhadap periferal pengguna dan lainnya, perangkat lunak Endpoint Management Data Loss Prevention (DLP), atau Pencegahan Kehilangan Data dengan Manajemen Titik Akhir, menyediakan sarana untuk menolak segala jenis akses ke port USB dan titik akses lainnya.



Sikap keamanan 'Blokir Semua Port' tentu dapat mengurangi risiko, dan, dalam beberapa keadaan, mungkin dibutuhkan, tetapi kebijakan tersebut sering kali terbukti menjadi instrumen yang sangat tidak efektif dengan konsekuensi yang tidak diinginkan.

Namun, beberapa administrator TI lebih memilih untuk menolak permintaan membuka port USB di komputer pengguna karena jka hal tersebut dilakukan di titik akhir akan memberikan akses langsung yang memintas keamanan firewall perusahaan. Tindakan hati-hati tersebut dapat dimengerti, tetapi dalam hal memberikan akses ke penyimpanan USB, penyediaan hak istimewa ini tidak harus menjadi masalah keamanan yang sangat besar jika beberapa prasyarat tertentu diikuti.

Salah satu persyaratan mendasar adalah paket aplikasi manajemen titik akhir yang memiliki fitur pemindaian pendeteksian ancaman pada solusi antivirus/anti-malware dan juga pemantauan serta manajemen terpusat terhadap semua titik akhir pengguna.

Umumnya, pendekatan yang langsung ini muncul dalam berbagai nama lain dalam solusi terpadu dari berbagai vendor populer, yang beberapa di antaranya adalah McAfee MVision, Sophos Intercept X, Symantec Endpoint Security, Trend Micro Smart Protection, dan WinMagic SecureDoc.

Perbaikan dalam pembuatan daftar putih (whitelisting)

Dalam hal pengamanan perangkat penyimpanan USB, metode yang diterapkan bergantung pada tingkat perlindungan yang diharuskan. Pendekatan sederhana tetapi efektif adalah dengan membuat daftar putih untuk perangkat penyimpanan USB dengan menggunakan nilai Pengidentifikasi Vendor (VID/Vendor Identifier) dan Pengidentifikasi Produk (PID/Product Identifier) pada masing-masing perangkat. Hal yang menarik tentang semua periferal USB adalah setiap produsen memiliki satu VID yang unik, tetapi dengan PID yang berubah-ubah untuk setiap produk baru yang dirilis.

Untuk keperluan pembuatan daftar putih, penggunaan VID produsen saja akan menjadi terlalu luas untuk tujuan keamanan karena berarti akan mengizinkan setiap perangkat USB yang diproduksi oleh produsen terkait. Penggunaan PID memberikan pembatasan yang lebih mendetail dengan mensyaratkan hanya model tertentu yang boleh diberi akses ke sistem host.

Meski hal ini suatu peningkatan, tetapi masih belum ideal. Perangkat penyimpanan USB sangat populer karena memungkinkan pengguna mendapatkan perangkatnya sendiri yang cocok dengan model yang diizinkan. Dengan memperhatikan hal-hal tersebut, Kingston Technology menawarkan solusi yang disesuaikan untuk memperketat keamanan perangkat penyimpanan USB.

Melalui program kustomisasi, tersedia layanan pembuatan profil PID khusus dan spesifik untuk suatu organisasi yang dapat diterapkan pada berbagai flash drive USB Kingston yang terenkripsi. Perusahaan yang menyebarkan perangkat berfitur pengidentifikasi produk yang disesuaikan tidak hanya mendapatkan manfaat dari kemudahan membuat daftar putih, tetapi juga peningkatan keamanan yang signifikan. Tanpa PID khusus yang cocok, meski terlihat identik, perangkat yang dibeli sendiri oleh karyawan akan ditolak aksesnya.

Meskipun penggunaan PID khusus akan mendukung pekerjaan administrator TI untuk lebih cepat dan mudah dalam memberikan akses ke perangkat penyimpanan USB, alternatif lain yang lebih mendetail adalah dengan menggunakan

nomor seri perangkat tersendiri yang menjadi fitur pada sebagian besar drive USB terenkripsi dari Kingston. Pengaturan ini mengharuskan setiap nomor seri perangkat yang unik didaftarkan pada paket manajemen titik akhir. Pada awalnya, pengaturan ini akan membutuhkan pemrosesan oleh staf TI, dan Kingston dapat menyertakan daftar nomor seri pada setiap pemesanan. Nomor seri tersebut selalu berbentuk alfanumerik dan tidak berurutan. Dengan memilih metode ini, kebijakan dapat dibuat jauh lebih fleksibel berdasarkan kepemilikan drive masing-masing dengan keunggulan tambahan pada akurasi penelusuran asal perangkat yang dapat menjadi sangat penting dalam skenario TI forensik. Sebagian drive Kingston menyertakan nomor seri dan barcode pada casing untuk pemindaian elektronik, dan drive lainnya dapat disesuaikan untuk penambahan barcode dan nomor seri pada casing sesuai kebutuhan bisnis; fitur ini dapat digunakan untuk pelacakan drive.

Secara default, sistem manajemen titik akhir menyediakan akses ke VID/PID untuk pemblokiran port dan pembuatan daftar putih. Penawaran Kingston memberikan cara yang lebih fleksibel untuk memaksimalkan penggunaan fitur-fitur tersebut sehingga memungkinkan kebijakan yang lebih akomodatif dan imajinatif untuk memudahkan penggunaan perangkat penyimpanan USB. Dengan menetapkan metode identifikasi yang tepat, sikap umum 'Blokir Semua Port' tidak hanya terlalu disederhanakan, tetapi juga tidak diperlukan lagi.

Solusi yang aman dan mematuhi aturan bagi pengguna jarak jauh

Dalam hal keamanan, pembuatan daftar putih perangkat hanya mengatasi separuh masalah, atau dengan kata lain, hanya separuh dari solusi.

Kemudahan dan kesederhanaan perangkat penyimpanan USB menjadikannya sulit digantikan di banyak perusahaan dan institusi yang mengutamakan portabilitas untuk melakukan transfer data tanpa masalah. Di sebagian besar lingkungan, untuk alasan kepatuhan dan higiene TI yang baik, staf perlu dilengkapi dengan drive USB terenkripsi untuk tugas tersebut. Dengan memanfaatkan kombinasi perlindungan kata sandi dan enkripsi perangkat, penyimpanan portabel dilengkapi dengan upaya perlindungan untuk mencegah akses ke data sensitif jika perangkat hilang, dicuri, atau ditinggalkan dalam situasi yang berpotensi rentan.

Ini bukanlah satu solusi untuk semua masalah karena teknik enkripsi dapat berbeda-beda, dan perbedaan paling signifikan terlihat saat membandingkan solusi enkripsi perangkat lunak dan perangkat keras. Jadi, mana yang lebih baik? Bergantung pada kebutuhan Anda, tetapi pertanyaan yang lebih tepat adalah, "Manakah yang lebih aman?"

Enkripsi perangkat lunak pada dasarnya adalah pilihan karena anggaran yang akan memenuhi kebutuhan beberapa sektor dengan operasi yang lebih kecil. Enkripsi ini juga sesuai untuk bisnis dengan transfer data yang dianggap tidak sensitif dan berfokus lebih pada kepatuhan kebijakan.

Namun, modus operandi enkripsi perangkat lunak juga merupakan kelemahannya karena membutuhkan aplikasi di sisi klien yang mengandalkan komputer untuk melakukan tugas enkripsi. Oleh karena itu, jika diasosiasikan, perangkat penyimpanan terenkripsi perangkat lunak hanya bisa seaman komputer host yang menggunakannya.

Eksposur pada eksploitasi juga meningkat karena peretas dengan akses ke memori komputer dapat "mengendus" kunci enkripsi/dekripsi. Data di drive juga dapat menjadi target serangan brute force karena perlindungan akses kata sandi tidak diperlukan jika file terenkripsi dapat diakses dan disalin.

Ingat bahwa enkripsi berbasis perangkat lunak mungkin membutuhkan pembaruan perangkat lunak dari waktu ke waktu yang dapat mempersulit pelaksanaan karena memberikan beban tambahan kepada staf TI. Hal terburuk dari semuanya, enkripsi perangkat lunak dapat dihapus sepenuhnya oleh karyawan yang merasa frustrasi atas masalah portabilitas drive di platform yang berbeda. Pengguna drive dapat menyalin data dari drive terenkripsi ke komputer, lalu memformat ulang drive menjadi drive tidak terenkripsi, kemudian menyalin kembali data semula ke drive. Pada tahap ini, data menjadi tanpa perlindungan dan sangat rentan terhadap pembobolan. Untuk tujuan kepatuhan terhadap undang-undang dan peraturan privasi data, metode tersebut tidak dapat diterima karena keamanan drive USB dapat dinonaktifkan dengan mudah.

Enkripsi pada chip: solusi yang sulit, tetapi cepat

Sebaliknya, drive USB terenkripsi perangkat keras akan berfungsi secara independen dari komputer karena memiliki prosesor khusus yang ditanam di dalam drive sebenarnya untuk mengelola enkripsi. Drive ini memiliki proses enkripsi yang selalu aktif dengan perlindungan terhadap serangan kata sandi brute force; data terenkripsi tidak dapat diakses dan tidak dapat disalin.

Drive USB terenkripsi perangkat keras tingkat perusahaan dan militer dari Kingston menggunakan enkripsi AES 256-bit dalam mode XTS. Sebagai teknik enkripsi yang telah diakui secara global, AES 256-bit menyediakan pengamanan data yang ketat. Dengan menggunakan dua kunci terpisah pada tahapan berbeda dalam proses enkripsi/dekripsi, mode XTS memiliki efek yang serupa dengan enkripsi dua kali pada data.

Dalam penggunaan, kunci enkripsi diturunkan dari alat penghasil nomor acak pada pengontrol drive yang dibuka dengan kata sandi pengguna. Karena autentikasi berlangsung di dalam perangkat keras-kriptografi perangkat, kunci enkripsi dan fungsi keamanan penting lainnya terlindungi dari eksploitasi umum seperti BadUSB, serangan cold boot, kode berbahaya, dan serangan brute force.

Salah satu manfaat langsung dari enkripsi perangkat keras adalah kinerja drive jauh lebih baik dibandingkan dengan drive terenkripsi perangkat lunak karena tidak ada pemindahan tugas enkripsi ke komputer host. Segala sesuatu berlangsung di dalam drive.

Drive USB yang terenkripsi perangkat keras seperti Kingston IronKey D500S adalah perangkat yang dilindungi oleh kata sandi yang terenkripsi secara bawaan. Dalam penggunaan, hanya volume peluncur yang tidak bisa ditulis yang terlihat sejak awal karena volume ini berisi aplikasi yang digunakan untuk melakukan autentikasi kata sandi dan membuka penguncian volume penyimpanan utama yang terenkripsi. Prosedur ini mencegah penginstalan driver atau perangkat lunak apa pun pada PC host.

Selain itu, drive USB terenkripsi perangkat keras Kingston berfitur firmware yang ditandatangani secara digital sehingga mencegah setiap manipulasi firmware di dalam perangkat. Memiliki lapisan keamanan tambahan ini memberikan perlindungan terhadap serangan seperti BadUSB yang mengeksploitasi kerentanan yang melekat pada firmware perangkat USB. Serangan ini dapat menyebabkan dijalankannya perintah atau kode berbahaya secara diam-diam pada komputer host.

Tentu saja, pendekatan 'Blokir Semua Port' akan membatasi risiko eksploitasi BadUSB, tetapi untuk apa mengorbankan produktivitas dengan praktik yang sudah ketinggalan zaman tersebut? Sebagaimana ditekankan di atas, lingkungan yang aman dapat dijaga bersamaan dengan penggunaan perangkat penyimpanan portabel jika disiapkan prosedur pengadaan dan penyebaran yang mudah untuk memperkenalkan drive USB terenkripsi perangkat keras.

Bekerja jarak jauh dengan aman dan mematuhi aturan

Untuk pekerja jarak jauh, berada jauh dari pengamanan lingkungan bekerja yang terlindung di organisasi menuntut perubahan strategi dan juga pandangan baru mengenai prioritas.

Dalam rencana keamanan bekerja jarak jauh, apakah menguntungkan jika port USB di laptop karyawan diblokir agar mereka dapat mengakses server melalui koneksi internet untuk mengunggah atau mengambil dokumen? Di tengah perjalanan, koneksi internet yang terbuka seperti titik akses Wi-Fi yang tidak aman atau tidak tepercaya mungkin satu-satunya yang tersedia bagi karyawan sehingga kondisi ini menimbulkan berbagai jenis bahaya yang sangat meningkatkan kemungkinan pembobolan data. Ancaman seperti intersepsi dan pengawasan data melalui spoofing

(pemalsuan), serangan Man-In-the-Middle (MitM), dan penyadapan jaringan hanyalah beberapa di antara berbagai metode peretasan yang makin canggih dan tersedia untuk penjahat dunia maya. Bahkan VPN juga pernah disusupi.

Koneksi jaringan organisasi ke internet sebenarnya adalah titik akhir yang lain. Paparan yang melekat pada koneksi tersebut menjadikannya titik masuk yang luar biasa rentan dan dijadikan target penyerangan. Membuka koneksi tersebut untuk akses jarak jauh menghadirkan risiko keamanannya sendiri, terutama untuk data yang sensitif.

Memberi pekerja jarak jauh drive USB terenkripsi perangkat keras dan terlindung kata sandi dapat secara efektif menurunkan potensi kerentanan jaringan. Namun, menyiapkan persediaan tersebut memerlukan pemeriksaan lebih lanjut terhadap drive USB yang tersedia dan cara drive USB tersebut dapat memenuhi tuntutan setiap lingkungan bekerja jarak jauh. Masalah ini tidak sesederhana seperti membuat pilihan perihal kapasitas drive atau apakah nomor seri drive harus tercatat. Masalah ini berkaitan dengan konstruksi fisik perangkat itu sendiri.

Perlindungan yang tahan tindakan manipulasi (tamper-proof): Opsi yang kuat

Masalah utama di sini adalah apakah drive USB terenkripsi perangkat keras tersebut tahan terhadap tindakan manipulasi (tamper-proof). Tingkat keamanan perangkat terhadap gangguan tersebut tercermin dalam standar seperti FIPS 140-3, yang memiliki beberapa tingkatan pemeriksaan ketahanan konstruksi fisik drive tanpa menggunakan metode kriptografi.

Sertifikasi FIPS-197 yang terkait hanya memperhatikan atribut dan perangkat enkripsi perangkat keras seperti SSD Eksternal seri IronKey Vault Privacy 50 dan Vault Privacy 80 yang merupakan model yang diorientasikan untuk perusahaan dengan persyaratan keamanan data yang di bawah persyaratan tingkat militer. Kedua drive tersebut lebih murah tetapi tidak memiliki perlindungan terhadap upaya manipulasi fisik pada drive.

Dengan sertifikasi FIPS 140-3 Level 3 (dalam proses), metode yang diterapkan untuk melindungi perangkat dari paparan manipulasi fisik dinilai berada pada tingkat militer. Kingston memasok berbagai drive berstandar FIPS 140-3 Level 3 ini ke berbagai perusahaan, instansi pemerintah, dan organisasi militer di seluruh dunia.

Menggunakan epoksi secara internal untuk melapisi semua sirkuit drive yang dibutuhkan untuk fungsi keamanan, kemudian merekatkan komponen internal tersebut ke casing perangkat, telah menciptakan lapisan pertahanan baru. Setiap upaya untuk membuka casing logam akan luar biasa sulit dilakukan dan akan menyebabkan kerusakan pada chip internal serta komponen lainnya sehingga pada akhirnya akan membuat drive tidak berfungsi. Dengan penambahan epoksi yang keras dan tidak tembus pandang ini, upaya manipulasi fisik terhadap komponen penting hampir mustahil untuk dilakukan. Perangkat seperti Kingston IronKey D500S dan S1000 telah dilengkapi dengan fitur keamanan tambahan ini.

Perlindungan pada perangkat ini tidak terbatas pada langkah pengamanan fisik saja. Kingston IronKey S1000 menghadirkan fitur ketahanan manipulasi ke tingkat yang lebih tinggi. Chip kriptografi internal IronKey S1000 dapat mendeteksi setiap upaya manipulasi fisik dan akan membuat drive tidak dapat digunakan begitu perangkat dinyalakan. Mengandalkan perangkat penyimpanan USB terenkripsi perangkat keras untuk mengakses dan mentransfer file sensitif adalah langkah pragmatis yang mempermudah pengoperasian jarak jauh yang tanpa hambatan dan secara efektif menjamin keamanan di lapangan.

Pastikan Anda menyelidiki perangkat keras dan fitur keamanan dari drive USB untuk mengetahui kemampuan perangkat tersebut dalam memenuhi kebutuhan spesifik dan kasus penggunaan Anda. Setiap drive USB harus ditinjau satu per satu dengan predikat akreditasi yang tepercaya guna membantu dalam pengambilan keputusan. Apa pun prioritasnya, Kingston menawarkan berbagai solusi drive USB terenkripsi perangkat keras dan opsi penyesuaian dengan harga yang terjangkau sehingga dapat mengatasi semua jenis lingkungan: mulai dari kepatuhan secara umum hingga tingkat paling tinggi, yakni spesifikasi militer tersulit.

Utamakan keselamatan: Tidak ada jaringan, tidak masalah

Saat ini, kantor tidak memiliki batasan tempat lagi. Seiringnya dengan terus berkembangnya model bekerja dari rumah, telah terjadi berbagai masalah kerentanan pada akses jarak jauh yang menjadi perhatian utama bagi banyak perusahaan. Banyak perusahaan menghadapi tantangan ini untuk pertama kalinya sehingga mencari cara lebih aman untuk mengakomodasi tren yang makin berkembang ini.

Untuk mendukung berbagai kebutuhan ini di berbagai jenis industri, perangkat penyimpanan USB terenkripsi perangkat keras sudah siap tersedia dan memberikan solusi yang aman untuk kondisi ketika transfer data melalui jaringan tidak bisa dilakukan atau tidak diinginkan karena beberapa alasan.

Di bidang keuangan, otoritas pelaksana peraturan sering kali meminta data untuk memeriksa perilaku dan kepatuhan suatu perusahaan. Risiko eksposur terlalu besar untuk mempertimbangkan penggunaan jaringan dalam mentransfer dokumen sensitif yang berisi informasi sangat detail tentang investasi, perdagangan pasar, dan aktivitas perbankan lainnya yang bersifat rahasia. Solusi yang sederhana dan efektif adalah dengan mengirimkan informasi tersebut di dalam drive USB terenkripsi perangkat keras.

Penggunaan drive USB yang terlindung untuk mentransfer file di lingkungan pelayanan kesehatan adalah kejadian sehari-hari. Cara ini digunakan untuk kemudahan bagi para dokter atau konsultan yang ingin menganalisis file, merujuknya untuk penelitian, atau mempresentasikan contoh kasus kepada mahasiswa kedokteran. Ada juga kebutuhan yang lebih praktis, yaitu dalam hal sistem terbatas milik pribadi seperti perangkat pencitraan medis yang memang tidak dilengkapi akses jaringan atau tidak menggunakannya untuk alasan keamanan. Dengan menggunakan drive USB terenkripsi perangkat keras yang mematuhi aturan, file dapat dengan mudah ditransfer untuk digunakan di tempat lain.

Hal yang boleh dan tidak boleh dilakukan

✓ **Gunakan drive yang terlindung dan mematuhi aturan** serta tinjau spesifikasinya untuk mendapatkan drive yang cocok dengan kebutuhan setiap penyebaran.

✗ **Jangan sahkan kebijakan Bawa Perangkat Anda Sendiri (BYOD) yang sembarangan atau personal** – untuk perusahaan apa pun, kehilangan drive yang tidak dienkripsi adalah kerugian yang terlalu tinggi dalam hal kerusakan finansial dan reputasi.

✓ **Sebarkan paket manajemen titik akhir** dan gunakan drive USB terenkripsi perangkat keras yang menawarkan fitur khas pembuatan daftar putih.

✗ **Jangan biarkan segala sesuatu terjadi karena kebetulan.** Evaluasi dengan tepat persyaratan untuk lingkungan kerja di tempat dan secara jarak jauh.

✓ **Berikan edukasi kepada staf** tentang persoalan keamanan. Para staf juga berkepentingan jika perusahaan tetap terlindung dari berbagai pelanggaran keamanan.

✗ **Jangan jadikan keamanan sebagai hal yang terlalu menyulitkan** sehingga pengguna mencari jalan pintas yang dapat mengakibatkan pemanfaatan solusi TI bayangan. Hanya karena suatu kebijakan umum selalu diterapkan, tidak berarti kebijakan tersebut cocok untuk semua skenario. Tempat bekerja selalu berubah dan dengan memilih solusi yang tepat, kebijakan baru dapat dibuat dan dilaksanakan.

Dalam skenario ini, Kingston Ironkey Keypad 200 (KP200) memperlihatkan kemampuannya dengan baik. Karena independen terhadap OS, drive ini tidak menggunakan volume peluncur untuk memasukkan kata sandi, melainkan berfitur keypad alfanumerik yang dapat membuka penguncian perangkat untuk digunakan di platform apa pun. Sebagai alat yang serba guna, drive USB terenkripsi perangkat keras digunakan meluas hingga ke bidang produksi; mentransfer dengan aman aplikasi yang dikembangkan di dunia penelitian dan pengembangan TI hingga mesin yang dikendalikan oleh platform teknologi operasional (OT). Untuk pengoperasian platform campuran yang juga berfitur Linux, KP200 adalah salah satu solusi terlindung yang paling sesuai dan tersedia.

Perangkat penyimpanan USB terenkripsi perangkat keras juga memiliki peran sangat penting dalam penegakan hukum. Perangkat USB tersebut melindungi dan dengan aman mentransfer file kasus, gambar-gambar, dan berbagai bukti lainnya ke petugas lapangan, regu investigasi, dan tim forensik. Kingston menawarkan manfaat tambahan karena dapat menyediakan drive dengan nomor seri internal yang tercetak pada casing eksternal bersama dengan barcode. Mendistribusikan dan membuat katalog drive menjadi tugas yang mudah dan gampang dilacak. Caranya semudah memasukkan nomor seri secara manual atau secepat memindai barcode – pengauditan dan manajemen persediaan menjadi sangat mudah. Fitur ini muncul sebagai standar pada drive Kingston IronKey D500S, D500SM, dan S1000B/E, tetapi juga tersedia untuk model terenkripsi perangkat keras lainnya sebagai bagian dari program Kustomisasi Kingston.

Keamanan dan mobilitas penyimpanan: Keadaaan terkini

Perlindungan kata sandi, enkripsi perangkat keras, perlindungan tahan manipulasi, pembuatan daftar putih titik akhir yang terperinci, sertifikasi FIPS 140-3 level 3 tingkat militer (dalam proses), dan pencatatan (logging) sekilas adalah berbagai fitur bawaan pada drive USB Kingston yang dapat disebarkan dengan sangat cepat.

Berbagai pertahanan keamanan yang kuat ini menjamin agar drive USB dan datanya tetap aman di lingkungan host yang menggunakannya. Meskipun spesifikasi yang tertulis sangat mengesankan, memilih model dengan acak tanpa penyelidikan apa pun belum tentu dapat memberikan solusi yang ideal bagi sebagian organisasi dengan persyaratan yang lebih rumit.

Sebagai produsen independen, Kingston menawarkan berbagai jenis pilihan untuk memenuhi kebutuhan pelanggan. Melalui program Kustomisasi Kingston, tersedia solusi tingkat lanjut, yang telah dirancang untuk memberikan pengalaman pengguna yang lancar.

Penyesuaian yang terlindung tidak sekadar memasok PID USB untuk tujuan pembuatan daftar putih bagi organisasi. Profil keamanan aplikasi peluncur juga dapat disesuaikan dengan menggunakan lima belas preferensi yang berbeda, mulai dari informasi kontak dan perusahaan hingga mengaktifkan petunjuk kata sandi serta menentukan jumlah maksimum percobaan kata sandi. Untuk eksternal, tersedia pencitraan merek (branding) perusahaan (logo bersama) serta berbagai pilihan warna untuk drive tertentu. Dengan pesanan minimum sebanyak lima puluh drive, semua fitur ini akan memberikan jalur integrasi yang mudah untuk penyebaran perangkat.

Jika aplikasi manajemen titik akhir yang sesuai untuk mengamankan penyimpanan USB belum tersedia, ada solusi manajemen yang tersedia bagi organisasi yang ingin mengelola seluruh aset drive Kingston mereka, termasuk opsi untuk mengatur ulang kata sandi secara jarak jauh.

Ketersediaan dan kemudahan USB telah membuatnya bertahan lebih lama dari berbagai teknologi yang menjanjikan, serta ketahanannya untuk berbagai tugas. Drive USB yang senantiasa tersedia, aman, dan terlindung menawarkan solusi sederhana yang dapat langsung dimanfaatkan.

Mengapa harus mengkhawatirkan pembobolan data jaringan di lingkungan bekerja jarak jauh? Dengan perangkat penyimpanan USB terenkripsi perangkat keras Kingston IronKey, jawaban untuk pertanyaan tersebut berada dalam genggaman Anda.

Untuk mempelajari selengkapnya tentang cara Kingston dapat membantu Anda, kunjungi kingston.com/ironkey atau untuk pertanyaan yang lebih spesifik, tanyakan kepada salah satu pakar USB Terenkripsi kami.

#KingstonIsWithYou #KingstonIronkey