Kingston TECHNOLOGY

Keamanan Optimal Endpoint Dijelaskan dan Dijelajahi dalam Kemitraan bersama Matrix42

MATRIX42

#KingstonIsWithYou

Keamanan Optimal Endpoint Dijelaskan dan Dijelajahi dalam Kemitraan bersama Matrix42

Pendahuluan

Perlindungan data adalah persyaratan dasar bagi bisnis, pemerintah, dan individu di zaman sekarang.

Pelanggaran data, peretasan, serta unsur manusia adalah ancaman dan risiko yang dialami di seluruh dunia. Kerugian finansial dan reputasi yang berkaitan dengan pelanggaran data bisa sangat besar. Persyaratan keamanan siber lanjutan dan strategi DLP endpoint (perlindungan kehilangan data) bergantung pada penyimpanan serta memori yang andal dan efisien.

Penggunaan enkripsi, memori serta penyimpanan yang cepat digabungkan dengan praktik terbaik, standar, dan kebijakan merupakan langkah yang penting. Kehilangan laptop serta drive USB dapat membuat individu maupun perusahaan sama-sama rentan terhadap pengungkapan informasi pribadi dan rahasia. Kingston menawarkan solusi pencegahan ancaman untuk membantu mitigasi risiko sekaligus melengkapi rencana keamanan yang ada atau yang sedang dikembangkan.

Keamanan Optimal Endpoint Dijelaskan dan Dijelajahi dalam Kemitraan bersama Matrix42

Isi

eBook singkat ini akan membahas solusi endpoint, lokasi USB drive terenkripsi, program kustomisasinya, serta perangkat lunak Matrix42 EgoSecure Data Protection yang telah membantu menyelesaikan enam tantangan sektor industri yang berbeda dan melengkapinya dengan solusi yang sesuai dengan kebutuhan bisnis mereka.

Kami menggali lebih dalam mengenai enam sektor ini dan mengamati cara mereka menangani tantangan keamanan endpoint.

Daftar isi

Bagian 1: Kasus Penggunaan Industri Sektor Publik

Situasi:

Di dalam sektor publik, penggunaan perangkat USB sangatlah umum. Contohnya, kantor dinas ketertiban umum harus menyalin foto yang diambil oleh pelanggar parkir dan pelanggaran administratif dari kamera digital ke sistem yang berwenang melalui kabel USB. Pihak kepolisian menerima data investigasi di perangkat penyimpanan data eksternal. Data ini perlu ditulis ulang dan dijaga dari akses yang tidak sah.

Tantangan:

Permintaan yang tinggi atas perangkat USB membuat karyawan rutin meminta drive USB. Penggunaan perangkat penyimpanan data yang bersifat pribadi dan tidak sah harus diblokir demi alasan keamanan. Jika karyawan membutuhkan perangkat penyimpanan USB baru, perangkat tersebut harus segera disediakan sesegera mungkin melalui Meja Bantuan Pengguna sehingga pekerjaan karyawan tidak terganggu. Penting untuk dicatat bahwa tidak ada masalah keamanan yang muncul dari penggunaan perangkat USB yang sesuai.

Solusi:

Dengan menggabungkan kontrol perangkat, penyaringan data, dan enkripsi, maka skenario berikut dapat terwujud:

Perangkat yang tidak diketahui secara umum diblokir di endpoint komputer. Perangkat penyimpanan data seperti kamera digital hanya diperbolehkan untuk fungsi tertentu seperti membaca file foto. Operasi tulis secara umum dienkripsi dan hanya diperbolehkan pada perangkat USB yang sah. Semua akses data dicatat. Manajemen perangkat yang sah dapat disederhanakan dengan cara menyesuaikan nomor seri dan ID perangkat keras. Jadi, Manajemen Layanan Matrix42 memungkinkan pengguna untuk meminta Drive USB Kington Technology yang dipersonalisasi pada Portal Layanan Mandiri. Setelah proses persetujuan, perangkat USB secara otomatis bisa digunakan di EgoSecure Data Protection.

> “Para karyawan kami sangat senang mengetahui bahwa perangkat USB baru dapat disediakan dengan mudah dan cepat setelah proses persetujuan yang singkat. Kami sangat senang dengan program kustomisasi dari Kingston Technology dan administrasi yang mudah dari kombinasi manajemen layanan dan keamanan endpoint milik Matrix42.”
>
> **Kepala Meja Bantuan, Sektor Publik**

Bagian 2: Kasus Penggunaan Industri Kesehatan

Situasi:

Perangkat layanan eksternal masih sering digunakan sebagai cara bertukar data antara karyawan dan institusi lain.

Misalnya, rumah sakit di Jerman harus menyediakan Registrasi Kanker dengan informasi tentang kasus kanker terkini serta perkembangannya. Untuk memudahkannya, data ini sering ditransfer melalui perangkat penyimpanan data seluler.

Para dokter juga suka menyimpan dokumen seperti data penelitian ke kuliah mereka melalui drive USB.

Tantangan:

Data pasien sangat sensitif dan tidak boleh jatuh ke tangan orang yang salah. Oleh karena itu, perlindungan data perlu ditingkatkan dan diperkuat. Jika pembawa data hilang, hal ini bisa menjadi masalah besar. Tidak hanya karena GDPR, tetapi juga kesehatan pasien. Karena alasan ini, penting untuk mengontrol, mengawasi, dan mengenkripsi akses ke penyimpanan data USB.

Solusi:

EgoSecure Data Protection menggabungkan berbagai tindakan perlindungan seperti kontrol akses, audit data, penyaringan, dan enkripsi ke dalam satu solusi. Administrator TI dapat memutuskan karyawan mana yang mendapat akses ke perangkat tertentu. Pengecualian dapat dibuat, contohnya dengan nomor seri dan ID perangkat keras. Tanda pengenal ini dapat ditentukan berkat program kustomisasi dari Kingston Technology sehingga hanya satu nilai yang perlu dikonfigurasikan di manajemen EgoSecure Data Protection untuk memungkinkan pelarangan penggunaan perangkat selain yang diizinkan perusahaan. Hal ini mengurangi upaya administrasi secara drastis serta meningkatkan keamanan data (GDPR, CCPA, HIPAA, dll), karena akses dienkripsi dan diawasi.

> “Kami telah menggunakan drive USB terenkripsi dari Kingston. Sekarang, dengan EgoSecure Data Protection, kami juga dapat memastikan bahwa kemudahan pelacakan dari transfer data pasien terwujud sesuai dengan EU-GDPR.”
>
> **CISO, University Hospital**

Bagian 3: Kasus Penggunaan Industri Keuangan

Situasi:

Bank tunduk kepada berbagai persyaratan kepatuhan. Salah satu persyaratannya adalah kepatuhan PCI-DSS (Standar Keamanan Data Industri Kartu Pembayaran). Persyaratan PCI-DSS termasuk kebutuhan atas enkripsi data, analisis kerentanan, dan penyaringan data. Tujuannya untuk mengurangi atau mencegah ancaman dan risiko keamanan TI sepenuhnya.

Tantangan:

Ada banyak risiko terkait dengan keamanan TI yang ada di endpoint. Karyawan harus menangani informasi kartu pembayaran dari konsumen dan bisnis, lalu mengolah data sensitif dari institusi keuangan setiap harinya. Oleh karena itu, mereka menghadapi ancaman berupa data dari cloud, email, USB, dan web yang dapat terpapar malware, atau data dapat tidak sengaja jatuh ke tangan pihak ketiga jika tidak cukup terlindungi. Insiden semacam itu dapat menjadi risiko dengan implikasi keuangan bagi sebuah bank, dalam hal GDPR, PCI-DSS, dan aturan perundangan Sarbanes-Oxley. Selain itu, penjahat siber mencoba untuk memengaruhi atau memanipulasi sistem perbankan dengan berbagai cara dan mereka akan lebih kreatif seiring berjalannya proses. Sebagai contoh, baru-baru ini terdapat kejahatan siber terkait ATM. Dalam rangka mencuri uang, mereka mengganggu pasokan daya dan sistem dinyalakan dengan perangkat USB yang dapat di-boot.

Solusi:

Sistem TI harus diamankan dengan tindakan pengamanan multi-lapis. Hal ini dapat dilakukan melalui kontrol aplikasi dan perangkat, deteksi anomali, UEBA (Analisis Tingkah Laku Entitas dan Pengguna), pengawasan serta enkripsi disk menyeluruh dengan Autentikasi PreBoot. Matrix42 dapat menjalankan ini dalam ekosistem terpadu dan terotomatisasi, sehingga hanya aplikasi berizin dan perangkat USB terenkripsi yang diperbolehkan. Selain itu, aktivitas yang mencurigakan atau berbahaya dideteksi, lalu tindakan selanjutnya dijalankan secara otomatis. Terkait dengan penggunaan drive USB, kombinasi dari drive USB terkustomisasi dari Kingston Technology membantu memastikan bahwa perangkat disertakan dalam daftar putih dengan upaya minimum dan data dienkripsi dengan cara yang mudah dilacak. Hal ini sangat meningkatkan kepatuhan dan tanpa upaya tambahan.

> “Dengan EgoSecure Data Protection dan fungsionalitas daftar putih, kami hanya mengizinkan drive USB terenkripsi dari Kingston. Kami memasukkan drive USB terenkripsi dari Kingston ke daftar putih dengan ID perangkat keras yang dipersonalisasi - perangkat lain tidak diizinkan. Hal ini secara drastis mengurangi upaya administrasi - dan meningkatkan keamanan!”
>
> **Manajer TI, Perusahaan Keuangan**

Bagian 4: Kasus Penggunaan Industri Otomotif

Situasi:

Dalam industri otomotif, penggunaan perangkat USB hadir di berbagai bidang. Sebagai contoh, data penelitian disimpan di perangkat penyimpanan eksternal dan dipertukarkan antar teknisi masing-masing perusahaan. Untuk mengonfigurasikan mesin produksi, file dipindahkan dari lingkungan TI ke lingkungan TO. Semua data ini sangat sensitif dan harus terlindung dari spionase industri dan pencurian data agar kekayaan intelektual yang dibangun tidak jatuh ke tangan yang salah.

Tantangan:

Industri otomotif tunduk kepada persyaratan kepatuhan seperti TISAX, perlindungan prototipe, ENX, ISO27001, "koneksi pihak ketiga", dan GDPR. Dalam TISAX, pasal Kontrol 9.1, 9.5, dan 10.1 mengatur bahwa akses data harus kontrol, diawasi, disaring, serta dienkripsi. Tindakan ini juga harus diperhatikan dalam persyaratan kepatuhan lainnya seperti GDPR dan ISO27001 di semua bidang perusahaan otomotif.

Solusi:

Drive USB terenkripsi dari Kingston Technology mengamankan data dengan enkripsi berbasis perangkat keras. Perangkat ini bisa mendapatkan nomor seri dan ID perangkat keras yang dipersonalisasi, yang dapat digunakan di EgoSecure Data Protection untuk dimasukkan ke daftar putih sebagai penggunaan data tertentu, secara otomatis. Selain itu, pergerakan data dapat diawasi dan dianalisis jika terdapat aktivitas yang mencurigakan.

> “Dengan Matrix42 dan Kingston Technology, kami mampu menerapkan persyaratan TISAX, misalnya Kontrol 9.5 (akses ke informasi dan aplikasi) dan Kontrol 10.1 (kriptografi) tanpa perubahan berarti dalam perilaku pengguna.”
>
> **CTO, pemasok otomotif**

Bagian 5: Kasus Penggunaan Industri Telekomunikasi

Situasi:

Telekomunikasi menyediakan banyak sekali informasi tentang pelanggan. Informasi ini sangat sensitif, khususnya yang berkaitan dengan GDPR. Selain itu, perlu adanya tindakan yang memadai untuk mencegah kehilangan dan pencurian data.

Tantangan:

Karyawan perusahaan telekomunikasi bekerja dengan data pelanggan setiap hari. Sebagian besar data disimpan di dalam aplikasi bisnis. Namun, ada risiko kontrak pelanggan atau ekspor basis data disimpan di endpoint dan perangkat eksternal yang tersambung dengannya. Untuk pertukaran data, pengguna sering menggunakan penyimpanan eksternal. Oleh karena itu, sangat penting untuk mendeteksi praktik penyimpanan data yang tidak tepat lalu mengoreksinya atau melindunginya.

Solusi:

Untuk menyederhanakan proses pembelian, drive USB terenkripsi dari Kingston Technology dengan ID Produk yang dipersonalisasi dapat dengan cepat dibeli melalui daftar putih yang ditentukan sebelumnya di EgoSecure Data Protection, lalu dikirim melalui Katalog Layanan Matrix42. Penyimpanan dan ekspor data dapat mengandung informasi sensitif. Hal itu bisa diidentifikasi secara otomatis serta diperbaiki dengan pengecekan konten mendalam berdasarkan pemindaian "data yang digunakan" dan "data yang tidak dipakai". Pergerakan data dicatat secara terpusat. Demikian, karyawan dapat menerima perangkat keras baru untuk penyimpanan data dengan cepat setelah diminta dan disetujui. Hal ini bisa menjamin kepatuhan terhadap GDPR.

> “Berkat portal layanan mandiri dari Matrix42, pengguna kami dapat meminta media penyimpanan yang mereka butuhkan. Setelah pesanan disetujui dan dikirim, perangkat diizinkan oleh kontrol perangkat dari EgoSecure. Kombinasi dari Matrix42 serta Kingston Technology meningkatkan produktivitas dan keamanan di perusahaan kami. ”

CTO, Penyedia Jasa Telekomunikasi

Bagian 6: Kasus Penggunaan Industri
Industri Manufaktur

Situasi:

Data digital adalah hal yang berharga di masa depan. Data yang bernilai di industri manufaktur ini mencakup rencana produksi, data tentang pelanggan dan pemasok, serta kekayaan intelektual perusahaan. Jika data ini hilang, tidak hanya dapat menyebabkan hukuman yang sangat berat dari sudut pandang GDPR, tetapi juga masalah eksponensial dan reputasi. Sayangnya, USB ditemukan di taksi, penatu, bandara, stasiun, atau tempat parkir setiap hari.

Tantangan:

Perangkat penyimpanan sering mengandung data yang sangat sensitif dan sayangnya, data ini sering tidak terenkripsi. Ada juga risiko mengenai teknisi servis menggunakan pembawa data eksternal untuk menginstal pembaruan bagi mesin produksi. Perangkat eksternal ini membawa risiko paparan malware ke dalam jaringan.

Solusi:

Drive USB terenkripsi dari Kingston Technology mengamankan data dengan enkripsi berbasis perangkat keras. Perangkat ini bisa dikirim dengan nomor seri dan ID perangkat keras yang dipersonalisasi, yang dapat digunakan di EgoSecure Data Protection untuk dimasukkan ke daftar putih sebagai penggunaan data tertentu, secara otomatis. Selain itu, pergerakan data dapat diawasi dan dianalisis jika terdapat aktivitas yang mencurigakan.

> “Sangat penting bagi kami untuk mengenkripsi data produksi untuk melindungi dari pencurian data. Data yang sangat sensitif ini hanya diperbolehkan di drive USB terenkripsi dari Kingston yang disetujui melalui penyaringan file oleh EgoSecure Data Protection. Pada semua perangkat USB lain, data produksi diblokir serta akses tulis ke penyimpanan data eksternal diamankan oleh enkripsi dan pencatatan dari Egosecure dengan cepat.”

Petugas Keamanan TI, Industri Manufaktur

Bagian 7: Solusi Kingston Technology dan Matrix42

Penggunaan enkripsi, memori serta penyimpanan yang cepat digabungkan dengan praktik terbaik, standar, dan kebijakan merupakan langkah yang penting. Kehilangan laptop serta drive USB dapat membuat individu maupun perusahaan sama-sama rentan terhadap pengungkapan informasi pribadi dan rahasia. Kingston Technology menawarkan solusi pencegahan ancaman untuk membantu mitigasi risiko sekaligus melengkapi rencana keamanan yang ada atau yang sedang dikembangkan.

Drive USB Terenkripsi dari Kingston Technology

Drive USB terenkripsi berbasis perangkat keras dari Kingston Technology menyediakan solusi perlindungan data untuk data seluler di dalam dan di luar firewall milik organisasi. Didesain untuk melindungi data yang membutuhkan pengamanan ketat, drive ini membantu Anda memenuhi standar, arahan, dan regulasi industri tertentu. Produk ini mematuhi TAA, bersertifikasi FIPS, dan tersedia dalam kapasitas hingga 128 GB, menjadikannya ideal untuk pengguna korporasi maupun agensi pemerintah.

Program Kustomisasi Aman

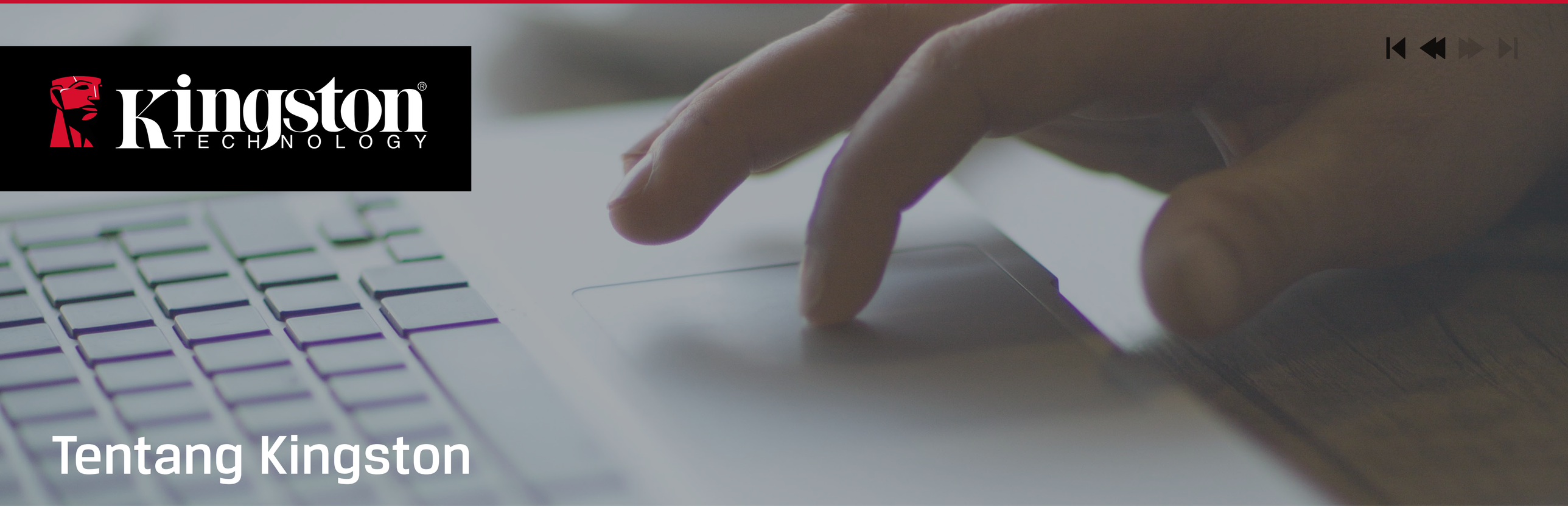
Anda dapat mengubah drive USB terenkripsi dari Kingston Technology dalam berbagai cara untuk memenuhi kebutuhan organisasi Anda. Tambahkan fitur yang dipilih untuk membuat drive yang unik dan satu-satunya. Kingston Technology menawarkan pemesanan yang mudah dan nyaman untuk drive USB terenkripsi yang dikustomisasi melalui retail pilihan Anda. Lini produk USB terenkripsi dari Kingston Technology termasuk seri DTVP30, DT4000G2, dan IKD300S. Program ini menawarkan pilihan yang paling sering diminta oleh pelanggan, termasuk penomoran seri, kata sandi ganda, dan logo kustom. Dengan pemesanan minimal 50 buah dan kuantitas pesan ulang sejumlah 25 buah, program ini memberikan persis seperti apa yang organisasi Anda butuhkan.

Matrix42 EgoSecure Data Protection

Matrix42 EgoSecure Data Protection menyediakan manajemen keamanan 360° bagi perusahaan untuk pencegahan serta perlindungan perangkat, sistem, dan data. Solusi ini mengotomatisasi keseluruhan proses. Mulai dari pencegahan dan deteksi hingga tindakan balasan saat terjadi kerusakan tanpa mengurangi produktivitas.

Ringkasan

Perlindungan data dan keamanan siber terasa seperti tanggung jawab yang menakutkan. Kebutuhan atas kerja digital telah berubah drastis bersamaan dengan kemampuan karyawan untuk memutuskan kapan, di mana, dan dengan perangkat apa mereka bekerja. Kombinasi yang tepat dari drive USB terenkripsi berbasis perangkat keras dan manajemen perangkat lunak endpoint dapat membantu organisasi untuk meraih kontrol perangkat organisasi mereka. Oleh karena itu, mengurangi risiko pelanggaran data dan mendukung strategi kepatuhan GDPR mereka yang sedang berlangsung.



Tentang Kingston

Dengan lebih dari 30 tahun pengalaman, Kingston Technology mempunyai pengetahuan untuk mengidentifikasi dan menyelesaikan tantangan keamanan endpoint tanpa mengorbankan organisasi Anda.

#KingstonIsWithYou