Kingston TECHNOLOGY

Optimale Endpoint Security, erklärt und erforscht in Partnerschaft mit Matrix42

MATRIX42

#KingstonIsWithYou

Optimale Endpoint Security, erklärt und erforscht in Partnerschaft mit Matrix42

Einführung

Der Datenschutz ist in der heutigen Zeit eine Grundanforderung für Unternehmen, Regierungen und Einzelpersonen.

Datenschutzverletzungen, Hacking und das menschliche Element erinnern ständig an weltweite Bedrohungen und Risiken. Sowohl die finanziellen Kosten als auch die Reputationskosten, die mit einer Datenverletzung verbunden sind, können astronomisch hoch sein. Die Anforderungen an fortschrittliche Cybersicherheit und Endpoint-DLP-Strategien (Schutz vor Datenverlust) beruhen alle auf zuverlässigem und effizientem Daten- und Arbeitsspeicher.

Der Einsatz von Verschlüsselung, schnellem Speicher und Arbeitsspeicher in Kombination mit Best Practices, Standards und Richtlinien ist ein großer Schritt. Verlorene Laptops und USB-Sticks machen Einzelpersonen und Unternehmen gleichermaßen anfällig für die Offenlegung persönlicher und privater Daten. Kingston bietet Lösungen zur präventiven Gefahrenabwehr, um Risiken zu minimieren und gleichzeitig einen bestehenden oder sich in Entwicklung befindlichen Sicherheitsplan zu ergänzen.

Optimale Endpoint Security, erklärt und erforscht in Partnerschaft mit Matrix42

Inhalt

Dieses kurze eBook befasst sich mit Endpoint Security Lösungen und zeigt, wie Kingston mit seinen verschlüsselten USB-Sticks, seinem Personalisierungsprogramm und der Matrix42 EgoSecure Datenschutz-Software sechs verschiedene Herausforderungen in sechs verschiedenen Branchen gelöst hat und ihnen eine Lösung liefert, die ihren Geschäftsanforderungen entspricht.

Wir beschäftigen uns eingehend mit diesen sechs Branchen und werden sehen, wie sie mit ihren Herausforderungen im Bereich der Endpoint Security umgegangen sind.

Inhaltsverzeichnis

Abschnitt 1: Branchenspezifischer Anwendungsfall Öffentlicher Sektor

Situation:

Im öffentlichen Sektor ist die Verwendung von USB-Geräten sehr verbreitet. So müssen beispielsweise Ordnungsämter die von Parksündern und Ordnungswidrigkeiten aufgenommenen Bilder von Digitalkameras über USB-Kabel auf die Systeme der Behörden kopieren. Die Polizeibehörden erhalten Untersuchungsdaten auf externen Datenspeichern. Diese Daten müssen neu beschrieben werden, und unbefugter Zugriff muss verhindert werden.

Herausforderung:

Aufgrund der hohen Nachfrage nach USB-Geräten fragen Mitarbeiter regelmäßig nach USB-Sticks. Die Verwendung privater und nicht autorisierter Datenspeichergeräte muss aus Sicherheitsgründen verhindert werden. Benötigt ein Mitarbeiter ein neues USB-Speichermedium, sollte dieses so schnell wie möglich über den Benutzer-Helpdesk zur Verfügung gestellt werden, damit die Mitarbeiter nicht bei ihrer Arbeit behindert werden. Dabei muss unbedingt darauf geachtet werden, dass durch die Verwendung der entsprechenden USB-Geräte keine Sicherheitsprobleme entstehen.

Lösung:

Durch die Kombination von Gerätekontrolle, Datenfilterung und Verschlüsselung kann Folgendes möglich gemacht werden:

Unbekannte Geräte werden in der Regel an Computer-Endpunkten blockiert. Datenspeichergeräte wie Digitalkameras sind nur für bestimmte Funktionen wie das Lesen von Bilddateien zugelassen. Schreibvorgänge sind generell verschlüsselt und nur auf autorisierten USB-Geräten zulässig. Alle Datenzugriffe werden protokolliert. Die Verwaltung von autorisierten Geräten kann durch die Anpassung von Seriennummern und Hardware-IDs vereinfacht werden. So ermöglicht das Matrix42 Service Management dem Benutzer, den personalisierten USB-Stick von Kingston Technology im Self-Service Portal anzufordern. Nach einem Genehmigungsprozess wird das USB-Gerät automatisch für die Verwendung in der EgoSecure Data Protection zugelassen.

> “Unsere Mitarbeiter sind begeistert von der Tatsache, dass neue USB-Geräte nach dem kurzen Genehmigungsverfahren einfach und schnell bereitgestellt werden. Wir sind sehr zufrieden mit dem Personalisierungsprogramm von Kingston Technology und der einfachen Verwaltung der Kombination aus Service-Management und Endgerätesicherheit von Matrix42.”
>
> **Leiter des Helpdesks, öffentlicher Sektor**

Abschnitt 2: Branchenspezifischer Anwendungsfall Gesundheitswesen

Situation:

Externe Speichergeräte werden nach wie vor häufig als Mittel zum Datenaustausch von Mitarbeitern und anderen Institutionen verwendet.

Beispielsweise müssen die Krankenhäuser in Deutschland dem Krebsregister Informationen über aktuelle Krebsfälle und deren Verlauf zur Verfügung stellen. Zur Vereinfachung werden diese Daten häufig über mobile Datenspeichergeräte übertragen.

Ärzte nehmen auch gerne Dokumente, wie Forschungsdaten, auf USB-Sticks zu ihren jeweiligen Vorlesungen mit.

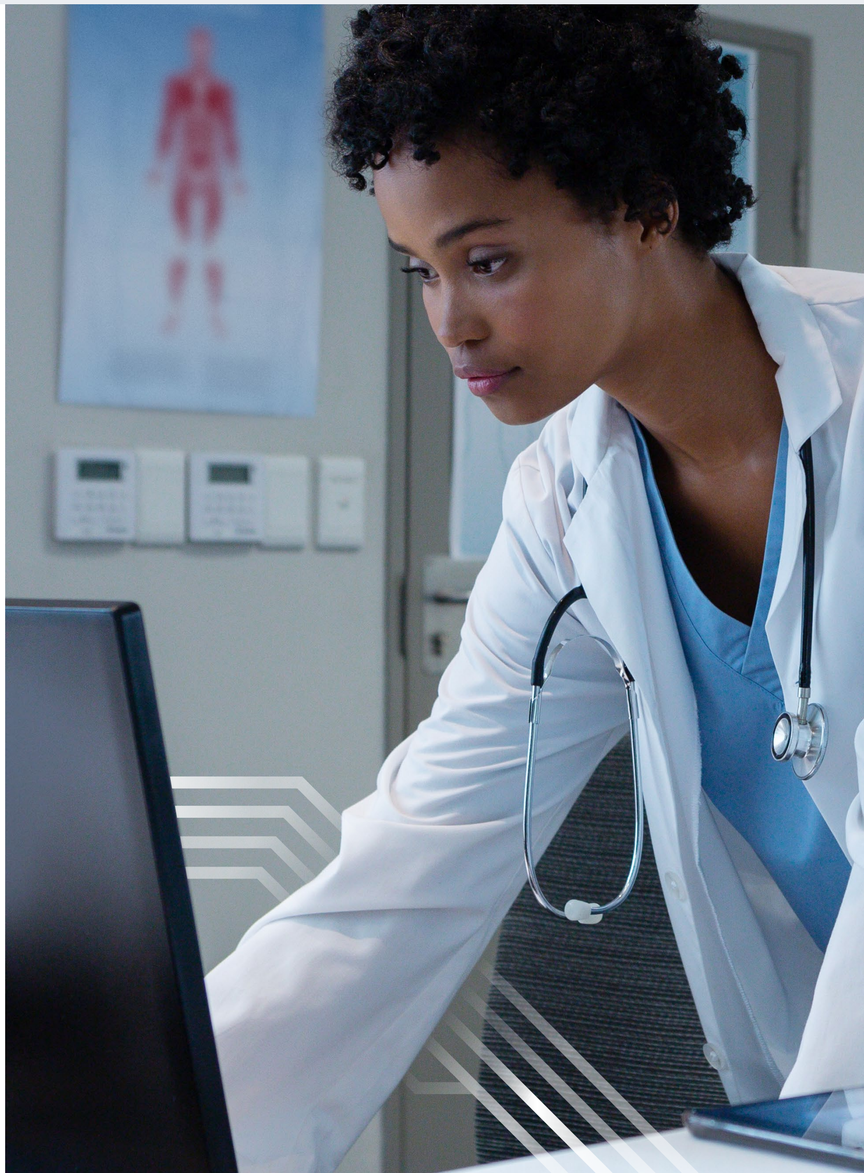
Herausforderung:

Patientendaten sind hochsensibel und dürfen nicht in die Hände Unbefugter gelangen. Daher muss der Datenschutz erhöht und gestärkt werden. Wenn ein Datenträger verloren geht, kann dies zu einem großen Problem werden, nicht nur wegen der DSGVO, sondern auch für das Wohl des Patienten. Deshalb ist es wichtig, dass der Zugriff auf USB-Datenspeicher kontrolliert, überwacht und verschlüsselt wird.

Lösung:

EgoSecure Data Protection kombiniert verschiedene Schutzmaßnahmen wie Zugriffskontrolle, Datenprüfung, Filterung und Verschlüsselung in einer Lösung. IT-Administratoren sind in der Lage zu entscheiden, welche Mitarbeiter Zugang zu welchen Geräten erhalten. Ausnahmen können z. B. nach Seriennummer und Hardware-ID gemacht werden. Diese Identifizierungsmerkmale können dank des Personalisierungsprogramms von Kingston Technology definiert werden, sodass nur ein Wert in der EgoSecure-Datenschutzverwaltung konfiguriert werden muss, damit nur vom Unternehmen genehmigte Geräte verwendet werden können. Dies minimiert den Verwaltungsaufwand sehr stark und erhöht die Datensicherheit (DSGVO, CCPA, HIPAA, etc.), da der Zugriff verschlüsselt und überwacht wird.

> “Wir hatten bereits verschlüsselte USB-Sticks von Kingston verwendet. Mit EgoSecure Data Protection können wir nun auch sicherstellen, dass die Rückverfolgbarkeit von Datentransfers von Patientendaten in Übereinstimmung mit der EU-DSGVO realisiert wird.”
>
> **CISO, Universitätsklinikum**



Abschnitt 3: Branchenspezifischer Anwendungsfall Finanzwesen

Situation:

Banken unterliegen verschiedenen Compliance-Anforderungen. Eine dieser Anforderungen ist die Einhaltung des PCI-DSS (Payment Card Industry Data Security Standard). Die Anforderungen des PCI-DSS umfassen die Notwendigkeit der Datenverschlüsselung, Schwachstellenanalyse und Datenfilterung. Ziel ist es, Bedrohungen und IT-Sicherheitsrisiken zu minimieren oder vollständig zu verhindern.

Herausforderung:

Es gibt viele Risiken für die IT-Sicherheit, die am Endpunkt bestehen. Mitarbeiter müssen täglich mit Zahlungskarteninformationen von Verbrauchern und Unternehmen arbeiten sowie sensible Daten von Finanzinstituten verarbeiten. Daher sind sie der Gefahr ausgesetzt, dass Daten aus der Cloud, aus E-Mails, USB-Geräten und dem Web durch Malware kompromittiert werden könnten oder, dass Daten versehentlich in die Hände Dritter gelangen könnten, wenn sie nicht ausreichend geschützt sind. Ein solcher Vorfall wäre ein Risiko mit finanziellen Auswirkungen für eine Bank in Bezug auf DSGVO, PCI-DSS, aber auch des Sarbanes-Oxley-Gesetzes. Darüber hinaus versuchen Cyberkriminelle, Bankensysteme auf verschiedene Weise zu beeinflussen oder zu manipulieren, und werden dabei immer kreativer. In jüngerer Zeit gab es zum Beispiel einen Cyberangriff im Zusammenhang mit Geldautomaten, bei dem die Stromversorgung unterbrochen wurde und das System mit einem bootfähigen USB-Gerät gestartet wurde, um Geld zu stehlen.

Lösung:

IT-Systeme müssen durch mehrschichtige Schutzmaßnahmen gesichert werden. Dies kann durch Anwendungskontrolle, Gerätekontrolle, Anomalieerkennung, UEBA (Benutzer- und Objektverhaltensanalysen), Überwachung und Festplattenverschlüsselung mit PreBoot-Authentifizierung erreicht werden. Matrix42 kann dies in einem automatisierten und integralen Ökosystem umsetzen, sodass nur zugelassene Anwendungen und verschlüsselte USB-Geräte zulässig sind. Darüber hinaus werden verdächtige oder böswillige Aktivitäten erkannt, und es werden automatisch weitere Maßnahmen eingeleitet. In Bezug auf die Verwendung von USB-Sticks trägt die Kombination von personalisierten USB-Sticks von Kingston Technology dazu bei, dass die Geräte mit minimalem Aufwand in die Whitelist aufgenommen werden und die Daten nachvollziehbar verschlüsselt werden. Dies erhöht die Compliance stark und ohne zusätzlichen Aufwand.

> “Mit EgoSecure Data Protection und der Whitelisting-Funktionalität lassen wir nur verschlüsselte USB-Sticks von Kingston zu. Wir führen verschlüsselte USB-Sticks von Kingston mit personalisierter Hardware-ID auf der Whitelist – andere Geräte sind nicht erlaubt. Das reduziert den Verwaltungsaufwand enorm – erhöht aber die Sicherheit!”
>
> **IT-Manager, Finanzunternehmen**

Abschnitt 4: Branchenspezifischer Anwendungsfall Automobilindustrie

Situation:

In der Automobilindustrie ist der Einsatz von USB-Geräten in verschiedenen Bereichen weit verbreitet. Beispielsweise werden Forschungsdaten auf externen Speichergeräten gespeichert und zwischen den jeweiligen Ingenieuren des Unternehmens ausgetauscht. Für die Konfiguration von Produktionsmaschinen werden Dateien von der IT-Umgebung in die OT-Umgebung transportiert. All diese Daten sind hochsensibel und müssen vor Wirtschaftsspionage und Datendiebstahl geschützt werden, sonst kann das aufgebaute Know-how in die falschen Hände geraten.

Herausforderung:

Die Automobilindustrie unterliegt Compliance-Anforderungen wie TISAX, Prototypenschutz, ENX, ISO27001, „Verbindung zu Drittanbietern" und der DSGVO. In der Richtlinie TISAX regeln die Artikel Control 9.1, 9.5 und 10.1, dass Datenzugriffe kontrolliert, überwacht, gefiltert und verschlüsselt werden müssen. Diese Maßnahmen sind auch bei den anderen Compliance-Anforderungen wie der DSGVO und ISO27001 in allen Bereichen von Automobilunternehmen zu beachten.

Lösung:

Verschlüsselte USB-Sticks von Kingston Technology sichern Daten mit hardwarebasierter Verschlüsselung. Diese Geräte können eine personalisierte Seriennummer und Hardware-ID erhalten, die in der EgoSecure Data Protection verwendet werden können, um für bestimmte Datenverwendungen automatisch auf die Whitelist gesetzt zu werden. Darüber hinaus können Datenbewegungen überwacht und analysiert werden, wenn es verdächtige Aktivitäten gibt.

> „Mit Matrix42 und Kingston Technology konnten wir TISAX-Anforderungen wie Control 9.5 (Zugang zu Informationen und Anwendungen) und Control 10.1 (Verschlüsselung) ohne größere Änderungen im Nutzerverhalten umsetzen."
>
> **CTO, Automobilzulieferer**

Abschnitt 5: Branchenspezifischer Anwendungsfall Telekommunikation

Situation:

Telekommunikationsanbieter verfügen über viele Informationen über ihre Kunden. Diese Informationen sind hochsensibel, insbesondere im Hinblick auf die DSGVO. Daher müssen ausreichende Maßnahmen ergriffen werden, um Datenverlust und Datendiebstahl zu verhindern.

Herausforderung:

Mitarbeiter von Telekommunikationsunternehmen arbeiten täglich mit Kundendaten. Die meisten Daten werden in Geschäftsanwendungen gespeichert. Es besteht jedoch das Risiko, dass Kundenverträge oder sogar Datenbankexporte auf Endgeräten und daran angeschlossenen externen Geräten gespeichert werden. Für den Datenaustausch nutzen die Benutzer häufig externe Speicher. Es ist daher sehr wichtig, dass falsche Praktiken der Datenspeicherung erkannt und korrigiert oder geschützt werden.

Lösung:

Für einen vereinfachten Beschaffungsprozess können verschlüsselte USB-Sticks von Kingston Technology mit einer personalisierten Produkt-ID schnell über eine vordefinierte Whitelist in EgoSecure Data Protection erworben und über den Matrix42 Service Catalog ausgeliefert werden. Datenspeicher und -exporte, die möglicherweise sensible Informationen enthalten, können automatisch identifiziert und durch eingehende Inhaltsprüfung auf der Grundlage von den Scans "Verwendete Daten" und "Daten in Ruhe" korrigiert werden. Datenbewegungen werden zentral protokolliert. So kann der Mitarbeiter neue Hardware für die Datenspeicherung schnell erhalten, nachdem diese beantragt und genehmigt wurde. Dies kann garantieren, dass der Vorgang DSGVO-konform ist.

> “Dank des Selbstbedienungs-Portals von Matrix42 können unsere Nutzer die benötigten Speichermedien anfordern. Sobald die Bestellung genehmigt und ausgeliefert ist, wird das Gerät durch die Gerätekontrolle von EgoSecure zugelassen. Die Kombination von Matrix42 und Kingston Technology erhöht die Produktivität und Sicherheit in unserem Unternehmen.”
>
> **CTO, Telekommunikationsanbieter**

Abschnitt 6: Branchenspezifischer Anwendungsfall Fertigungsindustrie

Situation:

Das Gold der Zukunft sind digitale Daten. Zu diesen wertvollen Daten in der Fertigungsindustrie gehören Produktionspläne, Daten über Kunden und Lieferanten sowie Firmen-Know-how. Wenn diese Daten verloren gehen, kann dies nicht nur zu sehr schweren Strafen im Hinblick auf die DSGVO führen, sondern auch zu exponentiellen und Reputationsproblemen. Leider findet man USB-Sticks täglich in Taxis, Wäschereien, auf Flughäfen, Bahnhöfen oder Parkplätzen.

Herausforderung:

Speichergeräte enthalten oft hochsensible Daten, und leider sind diese Daten oft nicht verschlüsselt. Es besteht ebenfalls das Risiko, dass Servicetechniker externe Datenträger verwenden, um Updates für Produktionsmaschinen zu installieren. Diese externen Geräte bergen das Risiko, Malware in das Netzwerk einzuschleusen.

Lösung:

Verschlüsselte USB-Sticks von Kingston Technology sichern Daten mit hardwarebasierter Verschlüsselung. Diese Geräte können mit personalisierter Seriennummer und Hardware-ID ausgeliefert werden, die in der EgoSecure Data Protection verwendet werden können, um für bestimmte Datenverwendungen automatisch auf die Whitelist gesetzt zu werden. Darüber hinaus können Datenbewegungen überwacht und analysiert werden, wenn es verdächtige Aktivitäten gibt.

> “Die Verschlüsselung unserer Produktionsdaten ist für uns sehr wichtig, damit wir uns vor Datendiebstahl schützen können. Diese hochsensiblen Daten sind nur auf zugelassenen verschlüsselten Kingston USB-Sticks mit Dateifilterung durch EgoSecure Data Protection erlaubt. Auf allen anderen USB-Geräten werden die Produktionsdaten blockiert und der Schreibzugriff auf externe Datenspeicher wird durch die On-the-Fly-Verschlüsselung und Protokollierung von EgoSecure gesichert.”

IT-Sicherheitsbeauftragter, Fertigungsindustrie

Abschnitt 7: Lösungen von Kingston Technology und Matrix42

Der Einsatz von Verschlüsselung, schnellem Speicher und Arbeitsspeicher in Kombination mit Best Practices, Standards und Richtlinien ist ein großer Schritt. Verlorene Laptops und USB-Sticks machen Einzelpersonen und Unternehmen gleichermaßen anfällig dafür, persönliche und private Daten zu exponieren. Kingston Technology bietet Lösungen zur präventiven Gefahrenabwehr, um Risiken zu minimieren und gleichzeitig einen bestehenden oder sich in Entwicklung befindlichen Sicherheitsplan zu ergänzen.

Verschlüsselte USB-Sticks von Kingston Technology

Die hardwarebasierten, verschlüsselten USB-Sticks von Kingston Technology bieten Datenschutzlösungen für mobile Daten innerhalb und außerhalb der Firewall einer Organisation. Diese Laufwerke wurden zum Schutz von Daten entwickelt, die eine lückenlose Sicherheit erfordern und helfen Ihnen, spezifische Industriestandards, Richtlinien und Vorschriften einzuhalten. Die Produkte sind TAA-konform, FIPS-zertifiziert und in Kapazitäten von bis zu 128GB erhältlich, sodass sie sowohl für Firmenanwender als auch für Regierungsbehörden ideal sind.

Sicheres Personalisierungs-programm

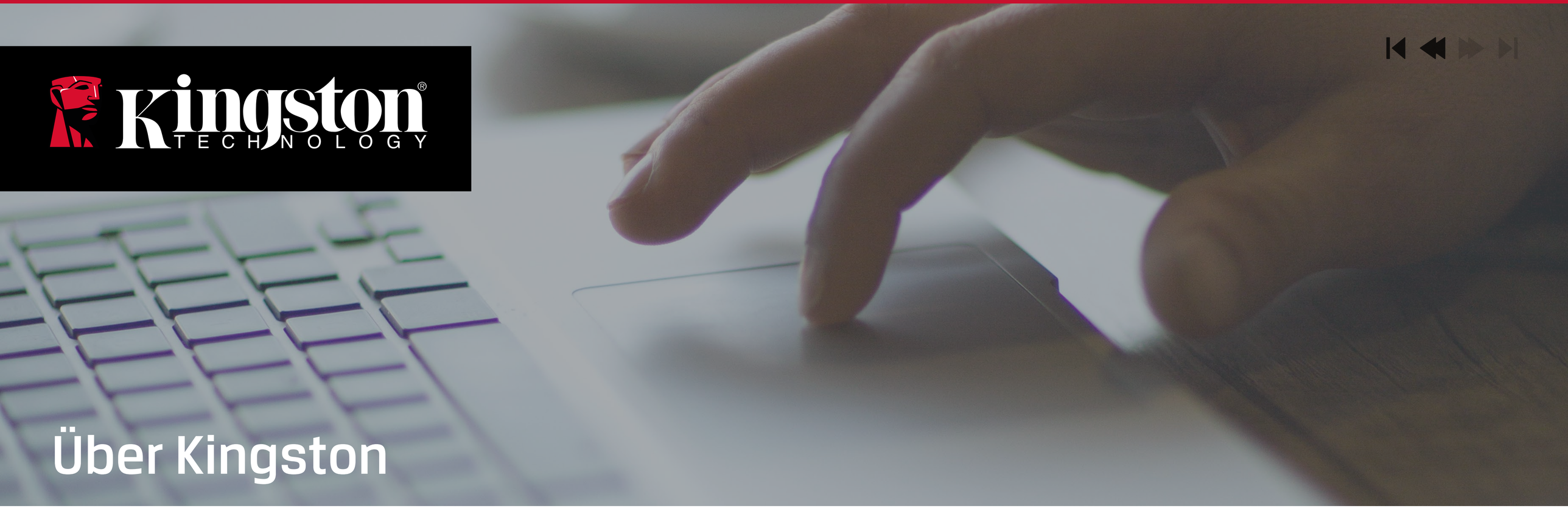
Ihnen stehen verschiedene Möglichkeiten zur Verfügung, verschlüsselte USB-Sticks von Kingston Technology den Bedürfnissen Ihrer Organisation anzupassen. Fügen Sie ausgewählte Funktionen hinzu, um einzigartige und unersetzliche USB-Sticks zu erstellen. Kingston Technology bietet eine einfache und bequeme Bestellung Ihres benutzerdefinierten verschlüsselten USB-Laufwerks über Ihren bevorzugten Händler. Zur Serie verschlüsselter USB-Produkte von Kingston Technology gehören die DTVP30, DT4000G2 und IKD300S Serie. In diesem Programm werden die von Kunden am häufigsten nachgefragten Optionen angeboten, einschließlich Seriennummerierung, dualem Passwort und benutzerdefinierten Logos. Schon bei einer Bestellmenge ab 50 Stück und einer Nachbestellmenge von 25 Stück liefert das Programm genau das, was Ihre Organisationen benötigt.

Matrix42 EgoSecure Data Protection

Matrix42 EgoSecure Data Protection bietet Unternehmen ein umfassendes 360°-Sicherheitsmanagement für die Prävention und den Schutz von Geräten, Systemen und Daten. Die Lösung automatisiert den gesamten Prozess von der Prävention und Erkennung bis hin zu Gegenmaßnahmen im Schadensfall ohne Produktivitätsverlust.

Fazit

Datenschutz und Cybersicherheit können wie eine gewaltige Verantwortung auf einem lasten. Die Anforderungen an die digitale Arbeit haben sich erheblich verändert, da die Mitarbeiter selbst entscheiden können, wann, wo und mit welchen Geräten sie arbeiten. Die richtige Kombination aus hardwarebasierten verschlüsselten USB-Sticks und Endpoint-Software-Management kann Unternehmen dabei helfen, die Kontrolle über die Geräte ihrer Organisation zu erlangen. ###Daher ist die Minimierung des Risikos von Datenverstößen und die Unterstützung ihrer laufenden DSGVO-Compliance-Strategie wichtig.



Über Kingston

Mit über 30 Jahren Erfahrung verfügt Kingston Technology über das Wissen, Ihre Herausforderungen im Bereich der Endgerätesicherheit zu erkennen und zu lösen, ohne Ihr Unternehmen zu gefährden.

#KingstonIsWithYou