SAMI ADVANCED ELECTRONICS
شركة الإلكترونيات المتقدمة

FORTRA™

تعزيز أمن البيانات وكفاءتها باستخدام خدمات نقل

الملفات المُدارة (MFT) وصمّامات البيانات

الملخص التنفيذي

مع الاعتماد المتزايد على البيانات، تواجه المنشآت تحديات متزايدة في نقل المعلومات الحسّاسة وعزلها بشكل آمن .

يُعدّ نقل الملفات المُدار (MFT) و صمّامات البيانات تقنيات مُتكاملة تُعالج هذه التحديات من خلال توفير حلول آمنة وفعّالة ومتوافقة لنقل البيانات وعزل الشبكات. يستكشف هذا التقرير التعاون بين نقل الملفات المُدار وصمّامات البيانات، وفوائدهما، ودورهما الحيوي في حماية البيانات الحسّاسة مع تسهيل العمليات التجارية.

المقدّمة

لقد أدى النمو الهائل لحجم البيانات ولتهديدات الأمن السيبراني المُتطورة إلى جعل نقل البيانات الآمن وعزل الشبكات من أهم أولويات المُنشآت في مختلف القطاعات، مثل النفط والغاز، والقطاعات المالية، والرعاية الصحية، والدفاع، ومختلف القطاعات الحكومية. وفي الحقيقة، فإن الطرق التقليدية، مثل البريد الإلكتروني وبروتوكول نقل الملفات (FTP)، لا تكفي لتلبية المتطلبات الأمنية والامتثال والكفاءة التشغيلية للمُنشآت الحديثة.

تقدم تقنيات نقل الملفات المُدار (MFT) وصمّامات البيانات حلولاً فعّالة تضمن تبادلاً آمناً وفعالاً للبيانات ومتوافقاً مع السياسات، وفي نفس الوقت تضمن الحد من مخاطر الاختراق والبرمجيات الضارة. نقدم في هذه الورقة البيضاء رؤىً ثاقبة وتفاصيل ذات علاقة حول هذه التقنيات وكيفية الاستفادة منها معاً لتلبية الاحتياجات الحسّاسة والحرجة لعالم الأعمال.

لمحة سريعة عن تقنية نقل الملفات المُدار (MFT)

يُعد نقل الملفات المُدار (MFT) حلاً أكثر أماناً وأتمتةً لنقل البيانات بين الأنظمة والأفراد والمُنشآت
وعلى عكس الطرق التقليدية، يُساعد نقل الملفات المُدار على ضمان أمان البيانات ووضوحها وتحقيق الامتثال من خلال عمليات التشفير وضوابط الوصول ومسارات التدقيق

الميزات الرئيسية لنقل الملفات المُدارة

عمليات نقل آمنة
تحمي عمليات التشفير والمصادقة البيانات أثناء النقل وأيضاً أثناء التوقف

الأتمتة
تُقلل عمليات النقل المُجدولة والمُدارة بالأحداث من التدخل اليدوي المُعرّض للأخطاء

قابلية التوسع
يُعالج كميات كبيرة من البيانات عبر نقاط نهاية متعدّدة

الامتثال
يُساعد المُنشآت على الالتزام بالمعايير الخارجية مثل اللائحة العامة لحماية البيانات (GDPR) وقانون النقل والمساءلة الخاص بالتأمين الصحي (HIPAA) ومعايير أمان بيانات قطاع بطاقات الدفع الإلكترونية (PCI DSS) وسياسة الإدارة الداخلية

حالات استخدام صمّامات البيانات

تبادل آمن للمعاملات المالية في القطاع المصرفي

مشاركة بيانات المرضى الحسّاسة في قطاع الرعاية الصحية

نقل البيانات التشغيلية في قطاعي النفط والغاز

لمحة سريعة عن صمّامات البيانات

صمّامات البيانات هي حلول أمنية قائمة على الأجهزة، تسمح بتدفق البيانات في اتجاه واحد، وتُساعد على ضمان عزل الشبكة. فهي تمنع الاتصالات ثنائية الاتجاه، ممّا يُقلل من خطر الهجمات السيبرانية من الشبكات الأقل أماناً

الميزات الرئيسية لصمّامات البيانات

إنتاجية عالية
ينقل كميات كبيرة من البيانات بكفاءة

تدفق بيانات أحادي الاتجاه
يُساعد على منع الهجمات الخارجية على الشبكات الحيوية

تصميم آمن من الفشل
يُساعد التنفيذ الفعلي لحركة البيانات في اتجاه واحد على ضمان عدم وجود أي ثغرات

التكامل
يتكامل بسلاسة مع بيئات تقنية المعلومات وتقنيات التشغيل الحالية

حالات استخدام صمّامات البيانات

حماية البنية التحتية الحيوية في قطاعي المرافق والطاقة

ضمان تصدير آمن للبيانات من الشبكات المصنّفة سرية إلى الشبكات غير السرية في قطاع الدفاع

عزل شبكات تقنيات التشغيل عن شبكات تقنية المعلومات في أنظمة التحكم الصناعية

لمحة سريعة عن بروتوكول تكييف محتوى الإنترنت (ICAP)

بروتوكول تكييف محتوى الإنترنت هو بروتوكول HTTP مُصمّم لنقل الملفات بكفاءة وأمان. يسمح تصميمه للأدوات بالتكامل مع الخدمات التي تُطبّق عمليات لاحقة. وقد أصبح هذا البروتوكول معياراً فعلياً لمرشحات المحتوى المُستضاف، مثل خدمات مكافحة البرمجيات الضارة وخدمات منع فقدان البيانات (DLP), وخدمات تصنيف بيانات Fortra (DCS) يسمح هذا لعمليات نقل الملفات بدمج إجراءات المسح لكلٍّ من عمليات النقل الواردة أو الصادرة

الميزات الرئيسية لبروتوكول تكييف محتوى الإنترنت

نقل أكثر أماناً للملفات
مسح وفحص الملفات باستخدام محركات مكافحة البرمجيات الضارة

تشفير SSL
يسمح بروتوكول تكييف محتوى الإنترنت عبر SSL بتشفير المحتوى أثناء نقله، مع التحقق من صحته

تعديل الاستجابة
تعديل المستندات لحظر المعلومات، وإزالة المحتوى النصي، وتحرير التفاصيل الحساسة، دون التأثير على البنية الأساسية للمستند

سياسات مسح وفحص البيانات
تعتمد نهجاً سياسياً يطابق سياسات الشركة لحظر أو عزل أو تعديل أو إصدار تنبيه بناءً على نتائج الفحص، مما يحمي بيئة التشغيل الخاصة بالمُنشأة

حالات استخدام بروتوكول تكييف محتوى الإنترنت

تطبيق عمليات مسح مدروسة وفورية حال دخول البيانات إلى الشبكة

تأمين البيانات أثناء نقلها، وعزلها أو حظر عمليات النقل إذا تم تقييمها على أنها غير آمنة

مراجعة وحماية تفاصيل الملكية الفكرية قبل خروجها من الشبكة

التكامل بين نقل الملفات المُدار وبروتوكول تكييف محتوى الإنترنت وصمّامات البيانات

بينما تضمن حلول خدمات نقل الملفات المُدارة وبروتوكول تكييف محتوى الإنترنت نقلاً آمناً وفعالاً للبيانات، توفر صمّامات البيانات عزلاً للشبكة. ومعاً، تُنشئان بنية أمنية متعددة الطبقات تحمي البيانات والأنظمة من التهديدات الخارجية والداخلية

المزايا المشتركة

أمان شامل

تُؤمّن خدمات نقل الملفات المُدارة البيانات أثناء النقل، بينما تعزل صمّامات البيانات الشبكات الحسّاسة والهامة

ضمان الامتثال

تدعم التقنيات المشتركة الامتثال التنظيمي من خلال حماية المعلومات الحسّاسة

استمرارية التشغيل

ضمان التبادل السلس للبيانات دون المساس بالأمان في البيئات المعزولة. وأيضاً ضمان إمكانية توصيل المعلومات، وتحديد إعادة المحاولة في حالة التوفر المؤقت للشبكة أو الأنظمة، وتلقي إشعارات فورية في حال عدم نقل بعض المعلومات ضمن النوافذ الخاصة لاتفاقيات مستوى الخدمة (SLA) المحدّدة. لا تفشل أبداً هذه المنظومة في تسليم أي ملف دون إشعار .

سلامة الملفات

ضمان عدم تعديل المعلومات من قِبل طرف ثالث في أي مرحلة من مراحل النقل باستخدام عمليات التحقق من المجموع الاختباري

قابلية التوسع

دعم النشر على نطاق واسع عبر بيئات متنوعة

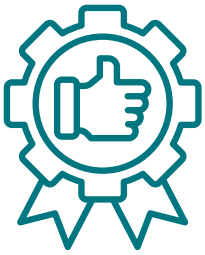
فحص متقدم للمحتوى

التحقق من المعلومات الواردة والصادرة من وإلى الشبكات الآمنة بحثاً عن أي محتوى نشط، أو فيروسات معروفة، أو ثغرات أمنية غير متوقعة، أو التحقق من نوع الملف، ويُطبَّق قواعد منع فقدان البيانات (DLP) على المحتويات التي تم تبادلها

إمكانيات التشفير

يُسمَح بالتشفير المزدوج عند الحاجة، ويُشفّر كلاً من قناة بروتوكول نقل الملفات الآمن (SFTP) عبر خوارزميات تشفير قوية بالإضافة للمحتوى، على سبيل المثال (PGP). بالإضافة إلى ضمان تشفير المعلومات في كل خطوة، حتى في العمليات المعقدة الشاملة من بدايتها إلى نهايتها

أفضل الممارسات العملية للتنفيذ



01. تقييم احتياجات العمل

تحديد تدفقات البيانات المهمّة والثغرات الأمنية المُحتملة

02. تحديد حالات الاستخدام

إعطاء الأولوية لحالات الاستخدام التي يُمكن فيها لخدمات نقل الملفات المُدارة وصمّامات البيانات تحقيق أقصى تأثير

03. تخطيط التكامل التقني

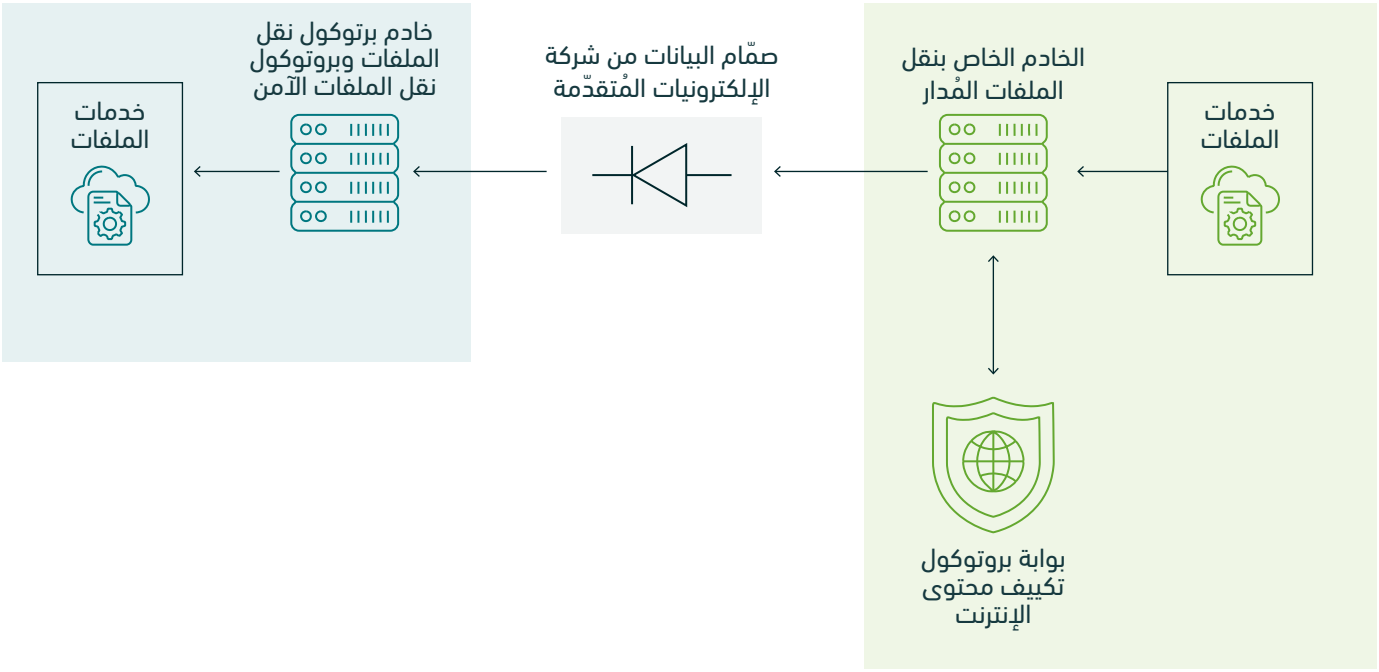
تصميم بنية حلول تدمج بين خدمات نقل الملفات المُدارة وصمّامات البيانات بسلاسة

04. الاختبار والتحقق

إجراء اختبارات شاملة لضمان تلبية الحلول لمتطلبات الأداء والأمان

05. المراقبة المستمرة

تدقيق ومراقبة عمليات نقل البيانات وآليات عزل الشبكة بانتظام



دراسة حالة

تعزيز أمن البيانات والامتثال لهيئة حكومية سعودية

نظرة عامة

احتاجت هيئة حكومية سعودية رائدة إلى طريقة آمنة وفعّالة لنقل البيانات الحسّاسة مع عزل الشبكات الحيوية والهامة. ومع وجود التهديدات الأمنية السيبرانية المتطورة ومتطلبات الامتثال الصارمة بموجب إرشادات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية، لجأت الهيئة إلى نظام نقل الملفات المُدار من Fortra، وصمّامات البيانات، وبوابة بروتوكول تكييف محتوى الإنترنت (ICAP) الآمنة من Clearswift لإنشاء إطار عمل شامل لأمن البيانات

التحديات

حماية البيانات
حماية البيانات السرية من التهديدات السيبرانية

عزل الشبكة
منع الوصول غير المصرح به إلى بيئات تقنية المعلومات وتقنيات التشغيل الحسّاسة

الامتثال التنظيمي
تلبية متطلبات الأمن السيبراني في المملكة العربية السعودية

الكفاءة
أتمتة عمليات تبادل البيانات الآمنة

الحل الذي تم تطبيقه

خدمات نقل الملفات المُدارة
عمليات نقل بيانات آمنة مع التشفير والأتمتة ومسارات التدقيق لضمان الامتثال

بوابة بروتوكول تكييف محتوى الإنترنت الآمنة من Clearswift
توفر فحصاً عميقاً للمحتوى (DCI)، ومنع فقدان البيانات (DLP)، وتصنيف البيانات من Fortra (DCS)، والحفاظ على البيانات لمنع اختراقها وضمان الامتثال عند تبادل الملفات

صمّامات البيانات
تضمن تدفقاً أحادي الاتجاه للبيانات، وعزلًا للشبكة، وإنتاجية عالية لمشاركة آمنة للبيانات عبر بيئات تقنيات التشغيل وتقنية المعلومات

أدى دمج حلول Fortra مع قدرات شركة الإلكترونيات المُتقدّمة إلى إنشاء بنية أمنية شاملة مصمّمة خصيصاً لحالات الاستخدام الحكومية ولحالات استخدام المُنشآت

النتائج

تعزيز الأمان
حماية البيانات بالتشفير، وعزل شبكات تقنيات التشغيل وتقنية المعلومات، والحفاظ على المعلومات الحساسة

الامتثال التنظيمي
استيفاء متطلبات الهيئة الوطنية للأمن السيبراني من خلال قدرات تدقيق قوية وضوابط منع فقدان البيانات وتصنيف البيانات

تحسين الكفاءة
قللت أتمتة سير العمل من التدخل اليدوي وحسّنت التعاون بين مختلف الأطراف

قابلية التوسع
دعمت أحجام البيانات المتزايدة مع توسع الهيئة في خدماتها الرقمية

الخلاصة

باستخدام خدمات نقل الملفات المُدارة (MFT) من Fortra، وصمّامات البيانات، وبوابة بروتوكول تكييف محتوى الإنترنت (ICAP) الآمنة من Clearswift، نجحت الهيئة الحكومية السعودية في تأمين بياناتها، وضمان الامتثال للوائح التنظيمية، وتعزيز كفاءتها التشغيلية. يدعم هذا الحل الشامل أهداف رؤية السعودية 2030 للتحول الرقمي والأمن السيبراني.

SAMI ADVANCED ELECTRONICS
شركة الإلكترونيات المتقدمة

FORTRA™

Contact Us

SAMI Advanced Electronics Company
King Khalid International Airport Industrial Estate
P.O. Box 90916,
Riyadh 11623, Saudi Arabia

+966112201350 **Email** - info@aecl.com

/AECSaudiArabia