الأمن السيبراني

(Zero Trust Model)

MAZAYA

SMART SYSTEMS SOLUTIONS

مزايا تحمي أعمالك بحلول سيبرانية ذكية

في عالمنا الرقمي، الأمن السيبراني عنصر أساسي لحماية بيانات الشركات واستمرارية أعمالها.
تقدّم مزايا حلولًا ذكية وموثوقة لمواجهة التهديدات الرقمية، مما يضمن تشغيلًا آمنًا وسلسًا، ويدعم صناع القرار في اتخاذ خطوات واثقة ومدروسة.

نموذج الأمان المعتمد على انعدام الثقة
Zero Trust

لماذا تحتاج المؤسسات إلى نموذج Zero Trust اليوم؟

- مع التحول الرقمي المتسارع وانتشار البيئات السحابية، لم تعد حلول الأمن التقليدية كافية.
- نموذج Zero Trust يلغي الثقة التلقائية ويتطلب التحقق المستمر من جميع محاولات الوصول.
- في مزايا، نعتمد إطار عمل Zero Trust لـJForrester كأساس لخدماتنا الأمنية.

الحلول التي نعتمدها
لحماية أعمالكم

1) Digital.ai

تطوير آمن وسريع للبرمجيات - Digital.ai

تُعد Digital.ai من الشركات الرائدة في تقديم حلول تقنية ذكية ومتكاملة في مجالات DevOps، وDevSecOps، وأمن التطبيقات.
تمكّن منصتها المؤسسات من تسليم البرمجيات بسرعة وكفاءة، مع حماية تطبيقات الهواتف الذكية والويب وسطح المكتب من التهديدات السيبرانية الحديثة.
كما تسهّل Digital.ai سير عمل DevOps وتُؤتمته، مما يُعزّز سرعة التطوير وكفاءة فرق العمل.
وتضمن قدراتها المتقدمة في DevSecOps تضمين الأمان في جميع مراحل دورة حياة تطوير البرمجيات.
في مزايا، نفخر بشراكتنا مع Digital.ai لتقديم حلول مرنة وآمنة لعملائنا، تُواكب متطلبات التحول الرقمي السريع وتضمن نجاحهم في بيئة رقمية متطورة.

2) نظام Scanwave

Scanwave System - الأمان الرقمي لأعمالك

تقدّم Scanwave System خدمات متكاملة في إدارة المخاطر الرقمية (RM) والاستشارات، مع تركيز خاص على الحوكمة، وإدارة المخاطر، والامتثال.
ومن خلال مواءمة استراتيجيات الأمن السيبراني مع أهداف العمل، تساعد المؤسسات على تعزيز مرونتها، والامتثال للأنظمة، والاستعداد لمواجهة التهديدات الرقمية المتجددة.
وبالتعاون مع Scanwave، نوفر في مزايا هذه الحلول الاستراتيجية لعملائنا، لتمكينهم من إدارة المخاطر بثقة وحماية مستقبلهم الرقمي.

3) Checkmarx

Checkmarx - أمن موحد للتطبيقات (SAST، SCA، DAST، IaC، مع فحص واجهات API)

في مزايا، تُمكّن المؤسسات من تأمين دورة حياة تطوير البرمجيات بالكامل من خلال شراكتنا الاستراتيجية مع Checkmarx، الشركة العالمية الرائدة في اختبار أمن التطبيقات (AST)
نقدّم نهجًا موحدًا لأمن التطبيقات يغطي جميع الطبقات: الكود المخصص، والمكونات مفتوحة المصدر، وواجهات البرمجة (APIs)، والبنية التحتية.
ومن خلال الاستفادة من القدرات المتقدمة لـ Checkmarx في مجالات SAST و SCA و DAST و IaC وأمن واجهات البرمجة، نضمن لعملائنا الحماية من التهديدات المتطوّرة، مع تسريع وتيرة التطوير.
وبفضل خبرتنا العميقة في السوق المحلي والتقنيات العالمية التي نوفرها، تساعد مزايا الشركات في المنطقة على بناء تطبيقات آمنة، ومتوافقة، ومرنة بسلاسة وعلى نطاق واسع.

4) ON2IT

إعادة تعريف الأمن السيبراني من خلال نموذج Zero Trust

من خلال شراكتها مع شركة ON2IT الرائدة في مجال أمن Zero Trust، تقدم مزايا حلول تكنولوجيا معلومات متكاملة تهدف إلى تعزيز الأداء التشغيلي وتأمين البيئات الرقمية. تشمل حلولنا البنية التحتية للشبكات، والأمن السيبراني، وخدمات الحوسبة السحابية، والاستشارات التقنية، وجميعها مصممة لتلبية احتياجات المؤسسات الحديثة المتطورة.
ومن خلال دمج إطار العمل المتقدم لنموذج Zero Trust من ON2IT مع خبرة مزايا الإقليمية، نساعد المؤسسات على تقوية موقفها الأمني، وتحسين قابلية التوسع، وتسريع التحول الرقمي.
وعبر الإدارة الاستباقية والتكامل الذكي، نُسهّل على المؤسسات تحسين بيئة تكنولوجيا المعلومات لديها بثقة وتحكّم كامل.

5) تقنيات GTB

GTB Technologies - سيطرة كاملة على أمن بياناتك

تُعد GTB Technologies شركة رائدة عالميًا في مجال الأمن السيبراني، ومتخصصة في حلول حماية البيانات المتقدمة التي تساعد المؤسسات على تأمين أصولها الحساسة، سواء في البيئات المحلية أو السحابية.
تتضمن منصتها أدوات قوية لاكتشاف وتصنيف البيانات، تُمكّن من تحديد وتصنيف المعلومات الحيوية بدقة، مما يشكّل الأساس لحوكمة فعّالة للبيانات.
كما توفّر قدرات رائدة في منع تسرب البيانات (DLP)، تتيح للمؤسسات منع الوصول أو مشاركة أو تسريب البيانات غير المصرح بها بشكل استباقي، مما يضمن الامتثال ويحمي الملكية الفكرية.
ولتأمين البيانات بشكل أعمق، تقدم GTB تقنيات العلامات المائية الرقمية التي تتبع البيانات الحساسة حتى خارج حدود المؤسسة، إلى جانب أدوات التحكم في الأجهزة والتطبيقات لضمان أن الأجهزة المصرح بها فقط يمكنها الوصول إلى المعلومات الحساسة.
في مزايا، نعتز بشراكتنا مع GTB Technologies لتقديم هذه الحلول القوية لعملائنا في المنطقة، ومساعدتهم على تحقيق الامتثال، ومنع الاختراقات، والحفاظ على رؤية وتحكم كاملين ببياناتهم في ظل المشهد الرقمي المعقّد اليوم.

6) Elastic

Elastic - بحث قابل للتوسع وذكاء سيبراني متقدّم

تُعد Elasticمنصة قوية مصمّمة لمعالجة تحديات البيانات الضخمة، حيث تقدّم أدوات متكاملة للرصد، وإدارة السجلات، والبحث، وذلك عبر محرك Elasticsearch عالي الأداء.
في مجال الأمن السيبراني، توفّر Elastic قدرات متقدمة في أنظمة إدارة معلومات الأمن (SIEM) وتحليلات الأمان، للكشف عن التهديدات والتحقيق فيها والاستجابة لها في الوقت الفعلي.
كما تشمل قدراتها الأمنية المحلية (On-Premises) أدوات كشف واستجابة للأجهزة الطرفية (EDR)للحماية من البرمجيات الخبيثة وهجمات الفدية، بالإضافة إلى استخدام الذكاء الاصطناعي والتعلّم الآلي للكشف التلقائي والدقيق عن التهديدات وتحليل الحالات الشاذة.
ومن خلال شراكتنا مع Elastic، تساعد مزايا المؤسسات على تسريع الوصول إلى الرؤى، وتأمين البنية التحتية، وتحديث عملياتها باستخدام تقنيات موثوقة من قِبل كبرى الشركات العالمية.

7) Ridge Security

يُعد هذا النظام منصة أمنية شاملة قائمة على السحابة، مصممة لتوفير حماية مستمرة لأعباء العمل السحابية والتطبيقات المعبّأة بالحاويات.
يعتمد على تقنيات الكشف الفوري عن التهديدات، وتحليلات السلوك، والاستجابة التلقائية لحماية التطبيقات طوال دورة حياتها.
ومن خلال تكامله مع بيئات DevOps والسحابة القائمة، يساعد المؤسسات على تقليل المخاطر الأمنية مع الحفاظ على المرونة والكفاءة التشغيلية.

8) FASOO

FASOO

FASOO - الاكتشاف، التصنيف، إدارة الحقوق الرقمية، العلامات المائية

تُعد Fasoo شركة رائدة عالميًا في أمن البيانات المحورية، وتقدم حلولًا متقدمة لحماية البيانات الحساسة غير المنظمة طوال دورة حياتها، من الإنشاء إلى المشاركة والتخزين.
تتميز منصتها بقدرات ذكية لاكتشاف وتصنيف البيانات، مع إمكانية وضع علامات وتشفير الملفات تلقائيًا لتبسيط الامتثال للتشريعات مثل GDPR hipaag

ومن خلال نظام إدارة الحقوق الرقمية (DRM)، تفرض Fasoo سياسات دقيقة للتحكم في الوصول والاستخدام، مما يضمن بقاء الملفات آمنة أينما ذهبت.

كما تتيح تقنيات العلامات المائية الديناميكية وتحليلات سلوك المستخدم للمؤسسات رؤية واضحة لاستخدام البيانات والحد من التهديدات الداخلية عبر تتبع وتحليل التفاعلات مع المحتوى المحمي.
في مزايا، نفخر بشراكتنا مع Fasoo لتقديم هذه القدرات المتطورة لعملائنا في المنطقة، ومساعدتهم على تحقيق تحكم كامل، وامتثال شامل، وثقة عالية في إدارة أصولهم المعلوماتية الحيوية.

9) Akamai

Akamai

يُعد هذا النظام منصة قوية لتسليم المحتوى وحماية السحابة، صُممت لتسريع توزيع المحتوى الرقمي للمستخدمين حول العالم.
يعتمد على شبكة واسعة من الخوادم الموزعة لتحسين أداء المواقع والتطبيقات، من خلال تقليل أوقات التحميل وتوفير وصول سريع وموثوق.
بالإضافة إلى ذلك، يوفّر حماية قوية ضد التهديدات السيبرانية مثل هجمات حجب الخدمة الموزعة (DDoS)، مما يساهم في تأمين الأصول الرقمية مع الحفاظ على تجربة مستخدم سلسة عبر مختلف الأجهزة والمواقع الجغرافية.

10) Wallarm

wallarm

هذا النظام هو منصة متقدمة قائمة على السحابة لحماية تطبيقات الويب وواجهات البرمجة (APIs) من مجموعة واسعة من التهديدات السيبرانية.
يستخدم تقنيات التعلّم الآلي وتحليل السلوك للكشف عن الهجمات وحظرها في الوقت الفعلي، مثل حقن SQL، والبرمجة عبر المواقع (XSS)، وسوء استخدام واجهات البرمجة.
ومن خلال تكامله السلس مع بيئات الحوسبة السحابية وسير عمل DevOps، يساعد المؤسسات على تحقيق أمان مستمر دون التأثير على أداء التطبيقات أو توفرها.

في مزايا، ندمج تقنيات عالمية المستوى لدفع التحول الرقمي وتعزيز الأمن السيبراني، مما يُمكّن المؤسسات من البقاء آمنة، مرنة، وجاهزة للمستقبل.

تواصل معنا اليوم واكتشف كيف يمكن لحلول مزايا السيبرانية أن تحمي مستقبلك الرقمي.

MAZAYA
SMART SOFTWARE SOLUTIONS

شكرًا !

www.mazayasolutions.com