BARDIN GATE

نقل آمن للبيانات بين الشبكات المعزولة

ART

AIR-GAP REGULATED TRANSFER

جهاز 2U يُركب في الحامل

الأمن والتشغيل: الجهاز والوكيل

من إعداد الجهاز إلى المفتاح على حاسوب المستخدم: الأمن يأتي من البنية، والتشغيل سهل بحكم التصميم، مع إعداد موجَّه وتحديثات موقّعة واسترداد بسيط.

في هذا الكتالوج: الوكيل بوصفه حدًا أمنيًا، وتركيب الجهاز، والتشغيل الأولي، والتحديث، والاسترداد

لمن: متخصصو الأمن وفريق التشغيل

https://www.bardin.tech/ar/bardingate-art/

في ART يشمل الحد الأمني حاسوب المستخدم إلى جانب جدار الجهاز. ولا يرث أي مكوّن الثقة من موقعه، وكل سلطة تتحقق من مدخلاتها.

تبقى شبكتاك منفصلتين ولا تتصلان ببعضهما ماديًا أبدًا؛ وجهاز 2U متصل بإحداهما فقط في أي لحظة.

عزل مادي

مفتاح مادي داخل الجهاز يصله بإحدى الشبكتين في كل مرة، ويفصل الأولى تمامًا قبل أن يصل الأخرى. عند كل تشغيل يُفصل كل شيء أولًا، وتُثبت حالة الفصل بتغذية راجعة من المفتاح نفسه، لا بمجرد أن أمرًا قد نُفّذ.

إقلاع موثوق

UEFI Secure Boot، وإقلاع مقيس في شريحة TPM 2.0، ونظام للقراءة فقط يُتحقق منه كتلةً كتلة بـ dm-verity. وسلسلة الإقلاع تُبنى مرة واحدة وهي نفسها على كل وحدة.

البيانات المخزنة

تُشفَّر البيانات منذ الإقلاع الأول بـ LUKS2 وAES-256-XTS. ولا يُفرج عن المفتاح إلا لإقلاع موقّع من المورّد، ويُعرض سرّ الاسترداد مرة واحدة على المُشغِّل الذي يجري التشغيل الأولي.

فحص معزول

تعمل المحللات ومحركات الفحص في حاويات دون root مع AppArmor وseccomp، دون شبكة، وبجذر للقراءة فقط وسقوف للموارد. وكل فشل ينتهي بالإغلاق.

الذكاء على الجهاز

يُحكم على الملف بحسب بايتاته الفعلية. نموذج ذكاء اصطناعي دون اتصال يوقف الملف ولا يمرّره أبدًا، والتدفق غير المعتاد يطلق تنبيهًا.

الوكيل حد أمني قائم بذاته

المفتاح والهوية

يُنشأ مفتاح الوكيل على الحاسوب نفسه ويُحفظ في المخزن الآمن لنظام التشغيل حيث توفّره المنصة. والتسجيل طلب شهادة مع موافقة صريحة من المسؤول، لا أثرًا جانبيًا لتثبيت ناجح أبدًا.

تخزين مؤقت مشفّر

النسخة المحلية لكل مستخدم مشفّرة بمفتاح محتوى يحميه المخزن الآمن لنظام التشغيل ومعزولة بقوائم التحكم في الوصول؛ ولا يستطيع مستخدم آخر على الحاسوب نفسه رؤيتها.

القناة

TLS 1.3 بهوية متبادلة. لكل مضيف وكيل شهادة جهاز خاصة قابلة للإلغاء؛ واسم المضيف أو عنوان IP ليس هوية أبدًا.

سلامة الملف

ملفات عادية فقط، دون تتبع الروابط؛ وبصمات في المصدر وفي التخزين المؤقت، وحصة، وجذور وجهات ثابتة، ونشر ذري، وقراءة نهائية من جديد. والمسار العشوائي لا يمنح أي سلطة أبدًا.

الهوية والوصول

- **الجهاز هو السلطة الوحيدة.** المتصفح والملفات المستوردة وكل ما عداها تأتي بادعاءات؛ ولا يستطيع أي منها منح سلطة.
- **الافتراضي هو المنع.** تحمل الأدوار نطاقًا صريحًا، والصلاحية غير المكتوبة رفض.
- **كلمة المرور، ثم كلمة المرور مرة أخرى.** الإجراءات عالية الخطورة (الأدوار، وسياسة الأمن، واستيراد الترخيص والتحديثات، وتصحيح الوقت، والاسترداد، واستيراد الإعدادات) تطلبها مرة أخرى.
- **لا باب خلفي.** لا كلمة مرور رئيسية للمورّد، ولا حساب مخفي، ولا استعادة عبر البريد، ولا تجاوز غير مسجَّل. واسترداد آخر مسؤول إجراء مادي أمام الوحدة.
- **لا يصل SSH إلا إلى حساب دعم مقيَّد.** يعيد التقارير والسجلات والحالة فقط؛ ولا دخول لـ root عبر SSH، ولا سطر أوامر للعمل اليومي ولا وصول مباشر إلى قاعدة البيانات.

الجهاز والتركيب

البند	ما يعنيه
الجهاز	جهاز بارتفاع 2U يُركب في الحامل، جاهز كما يُسلَّم. لا خادم ولا نظام تشغيل ولا برمجيات إضافية لاختيارها أو تثبيتها.
المساحة والكهرباء	مساحة 2U في حامل قياسي، وكهرباء.
الشبكة	اتصال بالشبكة الآمنة وغير الآمنة وشبكة الإدارة. ولا تتصل الأوليان ببعضهما أبدًا.
العمل اليومي	متصفح فقط. لوحة التحكم بأربع عشرة لغة، منها العربية.
الإنترنت	لا حاجة إليه؛ الترخيص والتحديثات والتواقيع تصل دون اتصال وموقّعة.

التدقيق وSIEM

الخاصية	القيمة
للإضافة فقط، ويكشف العبث	يُربط كل حدث ببصمة الحدث السابق؛ ويُغلق المقطع عند ١٠٬٠٠٠ حدث أو ساعة واحدة وتُوقَّع نقطة التحقق الخاصة به.
ما يُسجَّل	كل محاولة ونتيجة تخص الأمن والإدارة والأعمال الحرجة، مترابطة؛ بما فيها الإجراءات عالية الخطورة المرفوضة.
وقت موثوق	دون اتصال؛ يحافظ الجهاز بنفسه على ساعة الأمن، وخلل الساعة لا يمكنه تمديد ترخيص أو مهلة احتفاظ.
SIEM	تصدير منظَّم في اتجاه واحد إلى نظام SIEM لديك؛ TCP عبر TLS افتراضيًا، وmTLS اختياري، وRFC 5424 JSON أو CEF؛ والعناوين مستعارة. والنص الصريح أو UDP يتطلب تحذيرًا مقرًا به ومسجَّلًا في التدقيق.
ما لا يُصدَّر أبدًا	محتوى الملفات، وبيانات الاعتماد، والرموز المميزة، والمفاتيح الخاصة.

تشغيل أولي موجَّه

١ ركّبه
ركّب جهاز 2U ووصّل الكهرباء والشبكة الآمنة وغير الآمنة وشبكة الإدارة.

٢ افتح لوحة التحكم
افتح لوحة التحكم في المتصفح. يثبت رمزٌ على شاشة الجهاز نفسه أنك أمام الوحدة.

٣ إعداد موجَّه
تجري الخطوات بالترتيب وتختبر كل خطوة نفسها: العتاد، والوقت، وعناوين الشبكة، والمسؤول الأول.

٤ الاستلام
خذ حزمة أدلة التشغيل الأولي الموقّعة؛ الجهاز جاهز للعمل.

يتبع الوكيل: حزمة مؤسستك الموقّعة، ومفتاحًا يُنشأ على الحاسوب، وموافقة المسؤول على التسجيل، وحزمة إعدادات موقّعة من الجهاز. وتثبيت الوكيل ليس موافقة على تسجيله.

العمل اليومي: انظر، وافق، وهذا كل شيء

ينظر المسؤول إلى لوحة المعلومات ويوافق الموافِق على النقل. لا حاجة إلى SSH ولا نصوص برمجية؛ يعتني الجهاز بنفسه قدر استطاعته، وحيث لا يستطيع يخبرك بالسبب.

التحديث والتراجع

- **الحزم موقّعة وتعمل دون اتصال.** تُرفض الحزمة التي لا تحمل توقيعًا صالحًا أو تكون أقدم من تسلسل الإصدارات المسجَّل (منع الرجوع)؛ ويُمنع الرجوع العادي إلى إصدار أقدم.
- **قسمان للنظام.** يُكتب التحديث في القسم الآخر، ويُقلع منه مرة واحدة تجريبيًا، ولا يُعتمد إلا بعد نجاح فحوص السلامة؛ وإلا تعود الوحدة وحدها إلى الإصدار السابق.
- **البيانات منفصلة عن البرمجيات.** تصل تواقيع ClamAV وقواعد YARA ومخططات التحقق في حزمة بيانات فقط لا تغيّر البرمجيات أبدًا.

الاستبدال والاسترداد

الموقف	الطريق الصحيح
تعطل قرص واحد	استبدله وفق دليل التشغيل؛ تبقى وحدة التخزين سليمة أو قابلة للاسترداد.
مزوّد الطاقة أو المروحة	إجراء المورّد في وضع الصيانة، ثم إعادة التحقق من الجاهزية.
اللوحة الأم أو شريحة الأمان	يطلب الجهاز سرّ الاسترداد مرة واحدة، أمام الوحدة؛ ويحتفظ بهويته وإعداداته وترخيصه.
فقدان الجهاز بالكامل	جهاز بديل: تشغيل أولي جديد، واستيراد الإعدادات، وإدخال الأسرار من جديد، وإعادة إنشاء نقاط الاتصال. ولا تُستنسخ الهوية القديمة أبدًا.

الهدف الزمني للاستبدال	٨ ساعات من لحظة توفر العتاد والحزم والإعدادات والترخيص	**نقطة الاسترداد**	آخر تصدير موثَّق للإعدادات
ما لا يُستعاد	عمليات النقل الجارية، والمحتوى المحتفَظ به، والجلسات النشطة، والتدقيق الذي لم يُصدَّر قط	**المرسلون**	الطلب الذي لم يتلقَّ إيصالًا دائمًا يمكن إرساله من جديد

زمن الاسترداد هدف تصميمي، لا التزام مقيس؛ ويجب قياسه على جهازك قبل أي وعد تعاقدي.

الثقة لا تُورث من موقع مكوّن إلى آخر؛ فكل سلطة تتحقق من مدخلاتها.

كتالوجات أخرى لهذا المنتج

كتالوج ١
نظرة عامة على المنتج

كتالوج ٢
تجربة المستخدم

كتالوج ٣
فحص المحتوى

للاستشارة وطلب عرض توضيحي ومعلومات الاتصال:
https://www.bardin.tech/ar/bardingate-art/

قد تتغير المواصفات دون إشعار مسبق.