



ARP

AIR-GAP REGULATED PIPELINE



جهاز 2U يُركب في الحامل

الأمن والتشغيل: جهاز يعتني بنفسه

يأتي الأمن من بنية الجهاز، والتشغيل سهل بحكم التصميم: إعداد موجّه، وتحديثات موقّعة مع رجوع تلقائي، ووحدة تصلح نفسها.

في هذا الكتالوج: التشغيل الأولي، والتحديث والتراجع،
والإصلاح الذاتي، والاستبدال والاسترداد، وتركيب
الجهاز
لمن: متخصصو الأمن وفريق
التشغيل<https://www.bardin.tech/ar/bardingate-arp/>

أمن ARP ليس ميزة فوق المنتج؛ إنه بنية الجهاز. وإذا فشلت أي طبقة، يُغلق الجهاز بدل أن يستمر على خطأ.



تبقى شبكتك منفصلتين ولا تتصلان ببعضهما مادياً أبداً؛ وجهاز 2U متصل بإحدهما فقط في أي لحظة.

عزل مادي

مفتاح مادي داخل الجهاز يصله بإحدى الشبكتين في كل مرة، ويفصل الأولى تماماً قبل أن يصل الأخرى. عند كل تشغيل يُفصل كل شيء أولاً، وتثبت حالة الفصل بتغذية راجعة من المفتاح نفسه، لا بمجرد أن أمراً قد نُفذ.

إقلاع موثوق

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

البيانات المخزنة

تُشفّر البيانات منذ الإقلاع الأول بـ LUKS2 و AES-256-XTS. ولا يُفرج عن المفتاح إلا لإقلاع موقع من المورد، ويُعرض سرّ الاسترداد مرة واحدة على المُشغل الذي يجري التشغيل الأولي.

فحص معزول

تعمل المحلات ومحركات الفحص في حاويات دون root مع AppArmor و seccomp، 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 أبداً، والتدفق غير المعتاد يطلق تنبيهاً.



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 نطاقاً صريحاً، والصلاحيات 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 للمورد، ولا حساب مخفي، ولا استعادة عبر البريد، ولا تجاوز غير مسجل. واسترداد آخر مسؤول إجراء مادي أمام الوحدة.
- لا يصل SSH إلا إلى حساب دعم مقيّد. يعيد التقارير والسجلات والحالة فقط؛ ولا دخول ل root عبر SSH، ولا سطر أوامر للعمل اليومي ولا وصول مباشر إلى قاعدة البيانات.

التدقيق وSIEM

الخاصية	القيمة
الإضافة فقط، ويكشف العبث	يُربط كل حدث ببصمة الحدث السابق؛ ويُغلق المقطع عند ١٠,٠٠٠ حدث أو ساعة واحدة وتُوقّع نقطة التحقق الخاصة به.
ما يُسجّل	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، وخلال الساعة لا يمكنه تمديد ترخيص أو مهلة احتفاظ.
SIEM	تصدير منظم في اتجاه واحد إلى نظام SIEM لديك؛ TCP عبر TLS افتراضياً، و mTLS اختياري، و RFC 5424 JSON أو CEF؛ والعناوين مستعارة. والنص الصريح أو UDP يتطلب تحذيراً مقرأً به ومسجلاً في التدقيق.
ما لا يُصدّر أبداً	محتوى الملفات، وبيانات الاعتماد، والرموز المميزة، والمفاتيح الخاصة.

✦ العمل اليومي: انظر، وافق، وهذا كل شيء

ينظر المُشغل إلى لوحة المعلومات ويوافق الموافق. لا حاجة إلى SSH ولا نصوص برمجية ولا جداول؛ يعتني الجهاز بنفسه قدر استطاعته، وحيث لا يستطيع يخبرك بالسبب.



تشغيل أولي موجّه ✓

٤	الاستلام	٣	إعداد موجّه	٢	افتح لوحة التحكم	١	رغبه
خذ حزمة أدلة التشغيل الأولي الموقّعة؛ الجهاز جاهز للعمل.	تجري الخطوات بالترتيب وتختبر كل خطوة نفسها: العتاد، والوقت، وعناوين الشبكة، والمسؤول الأول.	افتح لوحة التحكم في المتصفح. يثبت رمزاً على شاشة الجهاز نفسه أنك أمام الوحدة.	رغب جهاز 2U ووصل الكهرباء والشبكة الآمنة وغير الآمنة وشبكة الإدارة.				

الإجراء مرتّب وإلزامي. ويُعرض سرّ استرداد القرص مرة واحدة، في صفحة التشغيل الأولي، للشخص الموجود أمام الوحدة.

التحديث والتراجع

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

الإصلاح الذاتي

يفترض الجهاز أن أحداً لا يستطيع الوصول إليه، فيصلح نفسه. لا محطة عمل ولا شاشة ولا SSH للعمل اليومي، ولا يجوز أن يتطلب أي تصميم للاسترداد الوصول إلى وحدة معطلة.

المستوى	ما تفعله	ما يبقى
إعادة ضبط مرنة	تعيد البرمجيات إلى آخر حالة سليمة معروفة؛ وهي الآلية نفسها التي يستخدمها رجوع التحديث.	الهوية والإعدادات والسجلات والتدقيق
إعادة ضبط كاملة	تعيد الوحدة إلى حالتها قبل التشغيل الأولي؛ فهي تمحو ولا تستعيد.	لا شيء؛ صدر التدقيق أولاً

الاستبدال والاسترداد

الموقف	الطريق الصحيح
تعطل قرص واحد	استبدله وفق دليل التشغيل؛ تبقى وحدة التخزين سليمة أو قابلة للاسترداد.
مزود الطاقة أو المروحة	إجراء المورد في وضع الصيانة، ثم إعادة التحقق من جاهزية.
اللوحة الأم أو شريحة الأمان	يطلب الجهاز سّر 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.

يحمل ملف إعدادات ARP كل المسارات والسياسات دون أي أسرار. وبعد استيراده لا يلزم إدخال مفاتيح SSH من جديد وتثبيت مفاتيح المضيفين من جديد.

الجهاز والتركيب

البند	ما يعنيه
الجهاز	جهاز بارتفاع 2U يُركب في الحامل، جاهز كما يُسلم. 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 والتوافيق تصل دون اتصال وموقع.

الجهاز الذي يجب أن يعمل حيث لا يصل إليه أحد عليه أن يصلح نفسه، وأن يعرف متى يجب ألا يستمر.

كتالوجات أخرى لهذا المنتج

كتالوج ٢

الفحص والحجر

كتالوج ٢

المسارات والسياسة

كتالوج ١

نظرة عامة على المنتج



للاستشارة وطلب عرض توضيحي ومعلومات الاتصال:

<https://www.bardin.tech/ar/bardingate-arp/>

قد تتغير المواصفات دون إشعار مسبق.