



ART

AIR-GAP REGULATED TRANSFER



2U اپلاینس رک مونت

امنیت و بهره‌برداری: هم دستگاه، هم Agent

از راه‌اندازی دستگاه تا کلید روی رایانه‌ی کاربر: امنیت از ساختار می‌آید و بهره‌برداری عمداً بی‌دردسر است؛ راه‌اندازی هدایت‌شده، به‌روزرسانی امضاشده و بازیابی ساده.

<https://www.bardin.tech/fa/bardingate-art/>

برای: متخصصان امنیت و تیم
بهره‌برداری

در این کاتالوگ: برنامه‌ی روی رایانه‌ی کاربر به‌عنوان رمز
امنیتی، نصب دستگاه، راه‌اندازی، به‌روزرسانی و بازیابی

در ART رمز امنیتی علاوه بر دیوار دستگاه، رایانه‌ی کاربر را هم در بر می‌گیرد. هیچ جزئی از جایگاهش اعتماد به ارث نمی‌برد و هر مرجع ورودی خود را دوباره می‌سنجد.

شبکه‌ی امن



شبکه‌ی ناامن

دو شبکه‌ی شما از هم جدا می‌مانند و هیچ اتصال فیزیکی میانشان برقرار نمی‌شود؛ اپلاینس رک مونت 2U در هر لحظه فقط به یکی از آن‌ها وصل است.

جداسازی فیزیکی

یک کلید فیزیکی داخل دستگاه در هر لحظه فقط یکی از دو شبکه را وصل می‌کند و پیش از وصل کردن دیگری، اولی را کاملاً قطع می‌کند. در هر راه‌اندازی هم همه‌چیز نخست قطع است، و قطع‌بودن با بازخورد خود کلید اثبات می‌شود، نه با اینکه «فرمان اجرا شد».

راه‌اندازی مطمئن

UEFI Secure Boot، بوت اندازه‌گیری‌شده در تراشه‌ی TPM 2.0 و سیستم فقط‌خواندنی که بلوک‌به‌بلوک با dm-verity راستی‌آزمایی می‌شود. زنجیره‌ی بوت یک‌بار ساخته می‌شود و روی همه‌ی دستگاه‌ها یکسان است.

داده‌ی ذخیره‌شده

داده از نخستین بوت با LUKS2 و AES-256-XTS رمز می‌شود. کلید فقط برای راه‌اندازی امضاشده‌ی سازنده آزاد می‌شود و رمز بازیابی فقط یک بار به راه‌انداز نشان داده می‌شود.

بازرسی در فضای ایزوله

تجزیه‌گرها و موتورهای بازرسی در کانتینر بدون ریشه، با AppArmor، seccomp، بدون شبکه، ریشه‌ی فقط‌خواندنی و سقف منابع اجرا می‌شوند. هر خرابی به «بستن» ختم می‌شود.

هوشمندی روی دستگاه

فایل از روی بایت‌های واقعی‌اش سنجیده می‌شود. مدل هوش مصنوعی آفلاین فایل را نگه می‌دارد ولی هرگز رد نمی‌کند، و جریان غیرعادی هشدار می‌دهد.

Agent، مرز امنیتی خودش

انبار رمز شده

نسخه‌ی محلی هر کاربر با کلید محتوای محافظت‌شده در ذخیره‌ی امن سیستم‌عامل رمز و با ACL جدا می‌شود؛ کاربر دیگر همان رایانه آن را نمی‌بیند.

کلید و هویت

کلید Agent روی همان رایانه ساخته می‌شود و در ذخیره‌ی امن سیستم‌عامل می‌ماند، هر جا که پلتفرم بدهد. ثبت‌نام با درخواست امضای گواهی و تأیید صریح مدیر انجام می‌شود، نه با نصب موفق.

یکپارچگی فایل

فقط فایل معمولی، بدون دنبال‌کردن پیوند؛ هش مبدأ و انبار، سهمیه، پوشه‌ی مقصد ثابت، انتشار یکجا و خواندن دوباره‌ی فایل نهایی. مسیر دلخواه هرگز اختیار نمی‌دهد.

کانال

TLS 1.3 با هویت دو طرفه. هر میزبان Agent گواهی دستگاهی خود را دارد که قابل ابطال است؛ نام میزبان یا IP هیچ‌گاه هویت نیست.

هویت و دسترسی

- دستگاه تنها مرجع است. مرورگر، فایل‌های وارد شده و هر چیز دیگر فقط «ادعا» می‌آورند و هیچ‌کدام نمی‌توانند اختیار بدهند.
- پیش‌فرض، رد است. نقش‌ها با دامنه‌ی مشخص تعریف می‌شوند و هر مجوز نوشته، یک امتناع است.
- رمز عبور، و دوباره رمز. کارهای پرخطر (نقش‌ها، سیاست امنیتی، مجوز و به‌روزرسانی، اصلاح زمان، بازیابی، وارد کردن پیکربندی) رمز را دوباره می‌خواهند.
- هیچ در پشتی وجود ندارد. رمز مدیر سازنده، حساب پنهان، بازنشانی با ایمیل یا دور زدن بی‌ثبات نیست. بازیابی آخرین مدیر یک رویه‌ی فیزیکی در محل دستگاه است.
- SSH فقط یک حساب پشتیبانی محدود. فقط گزارش، لاگ و وضعیت را می‌دهد و ریشه SSH ندارد؛ پوسته‌ی عادی یا ورود مستقیم به پایگاه داده نیست.

دستگاه و نصب

بخش	توضیح
دستگاه	یک اپلاینس رک‌مونت 2U با همه‌چیز آماده. لازم نیست سرور، سیستم‌عامل یا نرم‌افزار جانبی انتخاب یا نصب کنید.
جا و برق	2U فضا در رک استاندارد و برق.
شبکه	اتصال به شبکه‌ی امن، شبکه‌ی ناامن و شبکه‌ی مدیریت. دو شبکه‌ی اول هیچ‌گاه به هم وصل نمی‌شوند.
کار روزمره	فقط یک مرورگر. کنسول به چهارده زبان است، از جمله فارسی.
اینترنت	لازم نیست؛ مجوز، به‌روزرسانی و امضاها آفلاین و امضا شده‌اند.

میزی و SIEM

ویژگی	مقدار
افزودنی و مقاوم در برابر دستکاری	هر رویداد به Hash قبلی زنجیر می‌شود؛ هر بخش با ۱۰,۰۰۰ رویداد یا یک ساعت بسته و نقطه‌ی بازرسی‌اش امضا می‌شود.
چه ثبت می‌شود	هر تلاش و نتیجه‌ی امنیتی، مدیریتی و حیاتی کسب‌وکار، با شناسه‌ی هم‌بسته؛ از جمله کارهای پرخطر رد شده.
زمان معتبر	آفلاین؛ ساعت امنیتی را خود دستگاه نگه می‌دارد و ناهنجاری ساعت نمی‌تواند مجوز یا مهلت نگهداری را دراز کند.
SIEM	خروجی یک‌طرفه و تایپ‌شده به SIEM شما؛ پیش‌فرض TCP روی TLS، mTLS اختیاری، قالب RFC 5424 JSON یا CEF؛ نشانی‌ها به‌صورت شبه‌نام. متن ساده یا UDP نیازمند هشدار تأیید شده و ثبت در ممیزی است.
آنچه هرگز صادر نمی‌شود	بایتهای فایل، رمز، توکن و کلید خصوصی.

راهنمایی اولیه، هدایت شده

<p>۱</p> <p>نصب در رک</p> <p>دستگاه 2U را در رک می‌گذارید و برق و اتصال به شبکه‌های امن، ناامن و مدیریت را وصل می‌کنید.</p>	<p>۲</p> <p>باز کردن کنسول</p> <p>کنسول را در مرورگر باز می‌کنید. کدی که روی نمایشگر خود دستگاه می‌بینید ثابت می‌کند شما کنار آن هستید.</p>	<p>۳</p> <p>راهنمایی هدایت شده</p> <p>گام‌ها به‌ترتیب اجرا می‌شوند و هر گام خودش را می‌آزماید: سخت‌افزار، زمان، نشانی‌های شبکه و نخستین مدیر.</p>	<p>۴</p> <p>پذیرش</p> <p>بسته‌ی مدرک امضاشده‌ی راهنمایی را می‌گیرید و دستگاه آماده‌ی کار است.</p>
--	--	--	--

پس از آن Agent نصب می‌شود: بسته‌ی امضاشده‌ی سازمان شما، کلید در رایانه ساخته می‌شود، مدیر ثبت‌نام را تأیید می‌کند و دستگاه بسته‌ی پیکربندی امضاشده‌ای می‌دهد. نصب شدن Agent، تأیید ثبت‌نام نیست.

✦ کار روزمره: دیدن، تأیید کردن، و بس

مدیر داشبورد را می‌بیند و تأییدکننده انتقال را تأیید می‌کند. نه SSH لازم است، نه اسکریپت؛ دستگاه تا جایی که بتواند خودش را می‌پاید و جایی که نتواند، با دلیل روشن به شما می‌گوید.

به روزرسانی و بازگشت

- **بسته‌ها امضا شده و آفلاین‌اند.** بسته‌ی بدون امضای معتبر یا با شماره‌ی نسخه‌ی پایین‌تر رد می‌شود (ضد بازگشت)؛ تنزل نسخه‌ی عادی ممنوع است.
- **دو اسلات.** به‌روزرسانی در اسلات دیگر نوشته می‌شود، یک‌بار آزمایشی بوت می‌شود و فقط پس از سلامت‌سنجی قطعی می‌گردد؛ در غیر این صورت دستگاه خودکار به نسخه‌ی قبلی برمی‌گردد.
- **داده جدا از نرم‌افزار.** امضای ClamAV، قاعده‌های YARA و طرح‌واره‌های اعتبارسنجی در بسته‌ی داده‌ی جداگانه می‌آیند که فقط داده است و نرم‌افزاری را عوض نمی‌کند.

جایگزینی و بازیابی

وضعیت	مسیر درست
خرابی یک دیسک	جایگزینی طبق دستورالعمل؛ حجم سالم یا قابل‌بازسازی می‌ماند.
منبع تغذیه یا فن	تعمیر طبق رویه‌ی سازنده در حالت نگهداری و بررسی دوباره‌ی آمادگی.
برد اصلی یا تراشه‌ی امنیتی	دستگاه یک‌بار رمز بازیابی را در محل می‌خواهد؛ هویت، پیکربندی و مجوز خود را نگه می‌دارد.
از دست رفتن کل دستگاه	دستگاه جایگزین: راه‌اندازی اولیه‌ی تازه، وارد کردن فایل پیکربندی، ورود دوباره‌ی رمزها و برقراری دوباره‌ی نقاط پایانی. هویت دستگاه قبلی کلون نمی‌شود.
هدف زمان جایگزینی	۸ ساعت از لحظه‌ی دردسترس بودن سخت‌افزار، بسته‌ها، پیکربندی و مجوز
بازیابی نمی‌شود	انتقال‌های در جریان، محتوای نگهداری‌شده، نشست‌ها و ممیزی صادرنشده
نقطه‌ی بازیابی	آخرین خروجی راستی‌آزمایی‌شده‌ی پیکربندی
فرستنده	درخواستی که رسید ماندگار نگرفته، می‌تواند دوباره ارسال شود

زمان بازیابی یک هدف طراحی است، نه تعهد اندازه‌گیری‌شده؛ پیش از هر تعهد قراردادی باید روی دستگاه شما سنجیده شود.

اعتماد از جایگاه یک جزء به جزء دیگر ارث نمی‌رسد؛ هر مرجع، ورودی خود را دوباره می‌سنجد.

کاتالوگ‌های دیگر این محصول

کاتالوگ ۳

تضمین محتوا

کاتالوگ ۲

تجربه‌ی کاربر

کاتالوگ ۱

معرفی محصول



برای مشاوره، درخواست نمایش و اطلاعات تماس:

<https://www.bardin.tech/fa/bardingate-art/>

مشخصات ممکن است بدون اطلاع قبلی تغییر کند.