



AMG

AIR-GAP MAIL GATEWAY



2U اپلاینس رک مونت

امنیت و ایزولاسیون: رله‌ای که هیچ‌چیز را باز نمی‌گذارد

همتاها، رمزنگاری، رازها، سخت‌سازی Postfix و حریم محتوا؛ روی دستگاهی که ایزولاسیون فیزیکی دو شبکه را حفظ می‌کند.

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

برای: متخصصان امنیت

در این کاتالوگ: امنیت اتصال، توقف کامل در هر خطا،
حریم محتوا و رویدادها برای سامانه‌ی پایش امنیتی

AMG یک نقطه‌ی ورود ایمیل است؛ پس سخت‌ترین سؤال امنیتی را پیش از همه می‌پرسد: چه کسی اجازه دارد به من وصل شود؟ پاسخ دو نشانی IP است، نه بیشتر. بقیه‌ی طراحی برای آن است که این پاسخ در طول عمر دستگاه بدون تغییر بماند.



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 سوییچ فیزیکی درون 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.

راهاندازی مطمئن

UEFI Secure Boot، بوت اندازه‌گیری‌شده در تراشه‌ی TPM 2.0 و سیستم فقط‌خواندنی که بلوک‌به‌بلوک راستی‌آزمایی می‌شود.

صف رمزشده

صف پایدار روی حجم داده‌ی رمزشده‌ی دستگاه است (LUKS2 و AES-256-XTS) و RAID یک خرابی دیسک را تحمل می‌کند.

Postfix سخت‌شده و مستقل

Podman بدون دسترسی root، فایل سیستم فقط‌خواندنی، AppArmor، seccomp، بدون اختیارات اضافه‌ی سیستم و با سقف منابع؛ فرایندی جدا از بقیه‌ی نرم‌افزار دستگاه.

رمزنگاری

کنسول فقط با TLS 1.3 کار می‌کند؛ امضاها ECDSA روی P-256 با SHA-256؛ رمز عبور با MD5، Argon2id، SHA-1، 3DES و RC4 هرگز به کار نمی‌روند.

همتلاها و رمزنگاری انتقال

کنترل	چگونه کار می‌کند
فهرست مجاز IP	فقط اتصال مستقیم از دو نشانی تنظیم شده پذیرفته می‌شود. هر نشانی یک IPv4 یا IPv6 عددی است؛ نام میزبان در فیلد نشانی رد می‌شود.
بدون DNS و MX	اتصال همیشه مستقیم به همان نشانی IP است. نام میزبان فقط هویت همتا و نام مورد انتظار در گواهی است.
حالت TLS	REQUIRED پیش فرض است و گواهی طرف مقابل را اجباراً اعتبارسنجی می‌کند. OPPORTUNISTIC و OFF نیازمند هشدار صریح و اعمال ممیزی شده‌اند.
SMTP AUTH و mTLS	اختیاری و جدا برای هر سو؛ گواهی، کلید و رمز فقط به صورت ارجاع به مخزن اسرار نگه داشته می‌شوند.
جهت	فقط از IP همتا؛ تغییر دادن پیام نمی‌تواند آن را عوض کند.

اسرار هیچ‌جای دیگری نیستند

کلید خصوصی و رمزها هرگز وارد فایل پیکربندی، لاگ، پایگاه داده، خروجی عیب‌یابی یا SIEM نمی‌شوند. فایل پیکربندی فقط نشانی آن‌ها را در مخزن اسرار دارد.

هر خطا، توقف

- همتای ناشناس، IP یکسان برای دو سو، هویت TLS نامعتبر، رمز لازم مفقود، جهت مبهم و پیکربندی مخدوش، همه رد می‌شوند.
- اعمال پیکربندی نخست آزموده (postfix check) و فقط در صورت سلامت فعال می‌شود؛ وگرنه برمی‌گردد.

حریم محتوا

- متن، پیوست و موضوع پیام در هیچ لاگ، شاخص، فراداده‌ی پایگاه‌داده یا رویداد SIEM نمی‌آید.
- نشانی فرستنده و گیرنده در SIEM پیش‌فرض یک شبه‌نام پایدار با نمایش ماسک‌شده است. «کامل» و «حذف‌شده» دو گزینه‌ی صریح‌اند و حالت «کامل» هشدار و ممیزی دارد.
- شبه‌نام با HMAC و کلید جداگانه‌ی مخزن اسرار ساخته می‌شود؛ هاش ساده‌ی بی‌نمک ممنوع است و چرخش کلید نسل تازه می‌سازد.

ساختر امنیتی در یک نگاه

همتا	دقیقاً دو، با IP ثابت و متفاوت	TLS	پیش‌فرض الزامی، با اعتبارسنجی گواهی
رله‌ی باز	هرگز	MX و DNS	هیچ پرسشی در زمان رله
اسرار	فقط ارجاع در پیکربندی	محتوای پیام	بی‌تغییر و در هیچ لاگ یا رویدادی نیست
اجرای Postfix	بدون دسترسی root، فقط خواندنی، seccomp و AppArmor	اتصال دو شبکه	هرگز؛ هیچ اتصال فیزیکی میان‌شان نیست

هویت و دسترسی

- **دستگاه تنها مرجع است.** مرورگر، فایل‌های واردشده 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 پایگاه‌داده نیست.

رویدادها برای SIEM

رویداد	چه زمانی صادر می‌شود
MAIL_ACCEPTED	پیام در صف ماندگار پذیرفته شد
MAIL_DELIVERED	MTA مقابله پیام را پذیرفت
MAIL_DEFERRED	تحويل موقتاً شکست خورد؛ دلیل ثابت و زمان تلاش بعدی دارد
MAIL_FAILED	شکست دائمی یا انقضا؛ DSN صادر شد

تحويل به SIEM یک‌طرفه است و خرابی SIEM پذیرش SMTP را نمی‌بندد. همه‌ی رویدادهای امنیتی و ممیزی نیز به‌طور پیش‌فرض صادر می‌شوند.

✦ امنیت بدون کار اضافه

همه‌ی این کنترل‌ها پیش‌فرض دستگاه‌اند و روشن تحويل می‌شوند؛ شما فقط نشانی دو هم‌تا و گواهی‌هایتان را وارد می‌کنید.

رله‌ای که فقط با دو نشانی حرف می‌زند، فقط با گواهی معتبر و هرگز درباره‌ی محتوا قضاوت نمی‌کند.

کاتالوگ‌های دیگر این محصول

کاتالوگ ۴

بهره‌برداری

کاتالوگ ۲

پیام و صف

کاتالوگ ۱

معرفی محصول



برای مشاوره، درخواست نمایش و اطلاعات تماس:
<https://www.bardin.tech/fa/bardingate-amg/>

مشخصات ممکن است بدون اطلاع قبلی تغییر کند.