GRAPH

شرکت دانش‌بنیان گراف

www.graph-inc.ir

معرفی محصولات کیوسک گراف

راهکار امنیتی گراف مبتنی بر تحلیل فایل

حملات سایبری هر روز پیچیده‌تر می‌شوند و مجرمان آنلاین روش‌ها و ویژگی‌های متنوعی برای سرقت اطلاعات یا ایجاد اختلال در زیرساخت‌های فناوری بکار می‌گیرند. انتقال فایل به داخل شبکه یکی از راه‌های آلوده‌سازی سیستم‌ها و سامانه‌های سازمان‌هاست. حتی ایزوله‌ترین شبکه‌ها هم از فایل‌های آلوده در امان نیستند.

شرکت دانش‌بنیان گراف برای غلبه بر تهدیدات امنیتی از سطوح عادی تا سطوح بالایی مانند تهدیدات مانای پیشرفته(APT)، حملات روز صفر و بدافزارهای پیچیده، راهکارهای متنوعی ارائه داده است. ماژول تحلیل فایل گراف (Graph-FAM) یکی از این راهکارهاست که به منظور تامین امنیت فایل‌های ورودی به شبکه سازمان کاربردهای مهمی دارد.

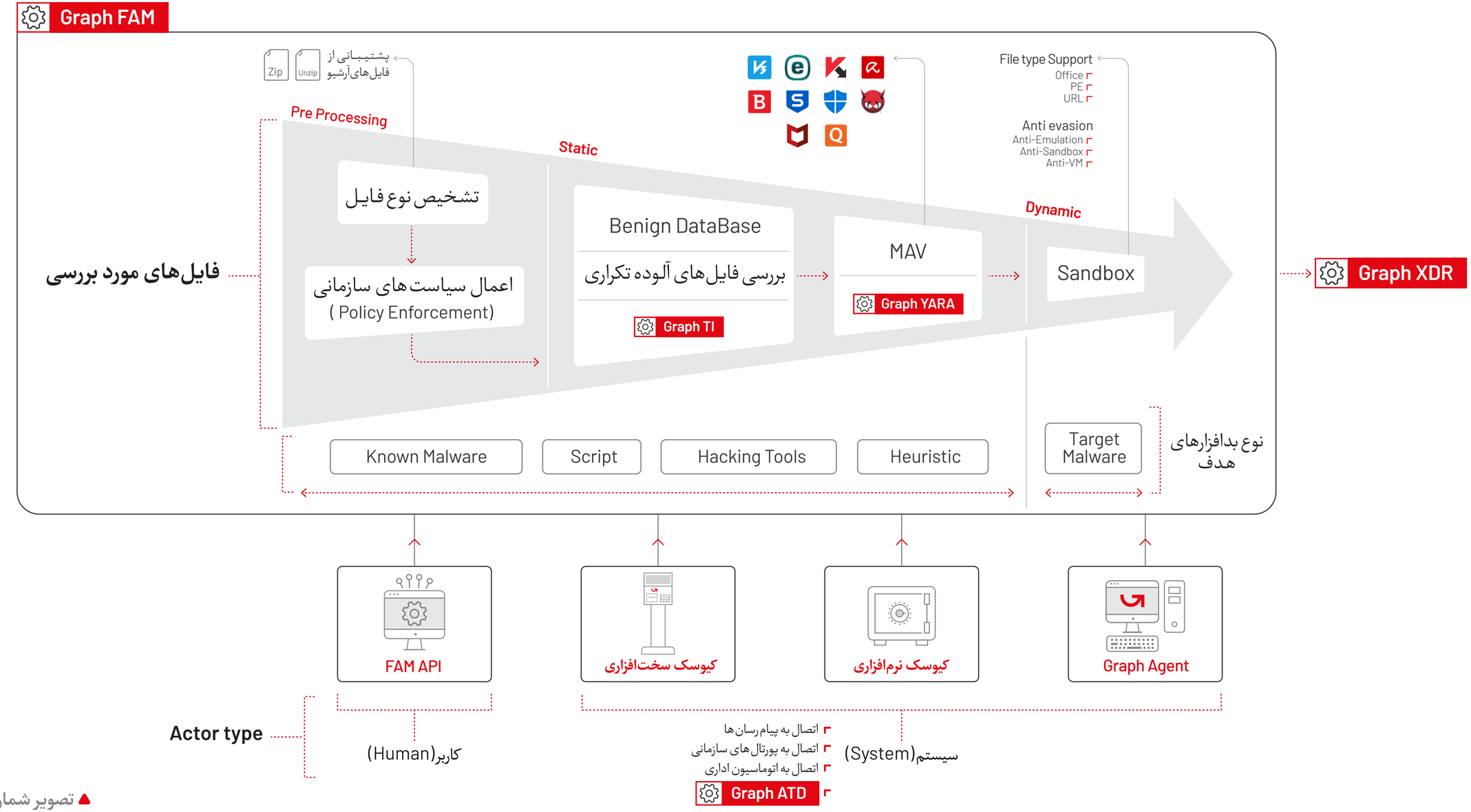
ماژول‌های موجود در محصولات کیوسک گراف

ماژول‌های مختلفی در کیوسک گراف وجود دارد که موارد اصلی آن به شرح زیر است:

- **موتور پردازشی چند آنتی‌ویروس (در دو نسخه‌ی ۵ آنتی‌ویروس و ۱۰ آنتی‌ویروس)**
- **موتور پردازشی YARA با قوانین اختصاصی شرکت گراف**
- **هوش تهدیدات گراف (Threat Intelligence Graph)**
- **اعمال سیاست‌های سازمانی (Policy Enforcement)**
- **موتور شناسایی نوع فایل براساس محتوی با قابلیت پشتیبانی از فایل‌های آرشیو و فشرده**

شرکت دانش‌بنیان گراف | تهران، شهرک سئول، دوم شرقی، شماره۴ | ۶۰۰۰ ۴۷۷۱ ۰۲۱

GraphFAM (File Analysis Module)



تصویر شماره ۱

شرکت دانش‌بنیان گراف | تهران، شهرک سئول، دوم شرقی، شماره۴ | ۶۰۰۰ ۴۷۷۱ ۰۲۱

راهکار امنیتی مبتنی بر فایل گراف، به صورت ماژولار ارائه می‌شود و در سطوح اطمینان و پیچیدگی متفاوت می‌تواند، از ورود فایل‌های مخرب به شبکه ایزوله یا عمومی سازمان جلوگیری کند. با اجرای فرآیندهای Graph-FAM شبکه سازمان تا ۹۸ درصد نسبت به ورود فایل‌های آلوده مصونیت پیدا می‌کند. در نهایت استفاده از سامانه XDR شرکت گراف می‌تواند تا ۹۹درصد از بروز حملات و تهدیدات سایبری جلوگیری کند.

نمایه سطوح اثربخشی سامانه تحلیل فایل

ماژول تحلیل	سطح خدمات گراف	درصد اثربخشی
MAV	بسته ۵ آنتی ویروس	۸۳٫۴۲ درصد
	بسته ۱۰ آنتی ویروس	۹۱٫۸۹درصد
YARA	موتور پردازشی YARA با قوانین اختصاصی شرکت گراف	۹۵٫۴۳درصد
TI	پایگاه داده هوش تهدید گراف	۹۷٫۸۹ درصد
Sandbox	سندباکس	۹۸ درصد
XDR	سامانه شناسایی تهدیدات پیشرفته گراف	۹۹ درصد

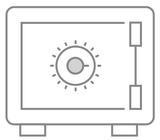
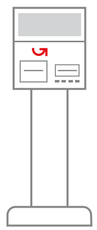
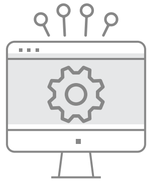
Graph FAM

Graph ATD

▲ تصویر شماره ۲

مدل‌های مختلف کیوسک گراف به عنوان مبادی ورودی، انواع فایل را برای بررسی به سامانه تحلیل فایل گراف منتقل می‌کنند. بعد از تحلیل فایل و تایید مجاز بودن آن، اجازه انتقال آن به شبکه‌های ایزوله و خصوصی داده می‌شود.

محصولات کیوسک گراف بر پایه فناوری ماژول تحلیل فایل گراف (Graph FAM) در چهار مدل زیر ارائه می‌شود:

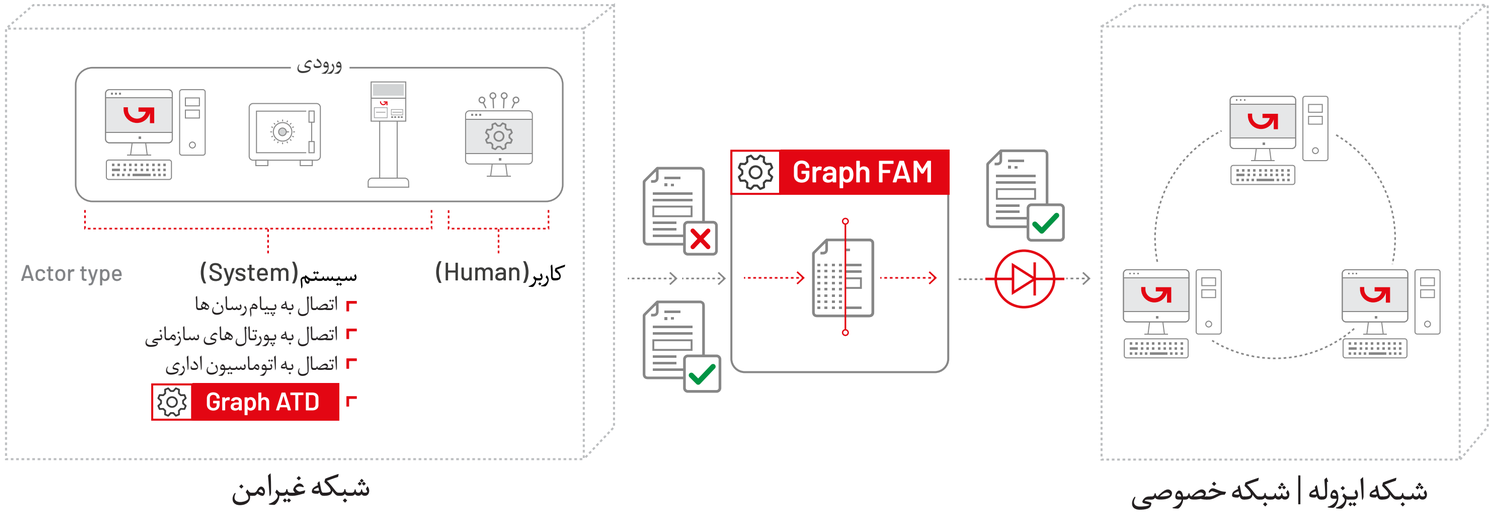
Graph Agent	کیوسک نرم‌افزاری	کیوسک سخت‌افزاری	FAM API
			 API

▲ تصویر شماره ۳

شرکت دانش‌بنیان گراف | تهران، شهرک سئول، دوم شرقی، شماره۴ | ۶۰۰۰ ۴۷۷۱ ۰۲۱

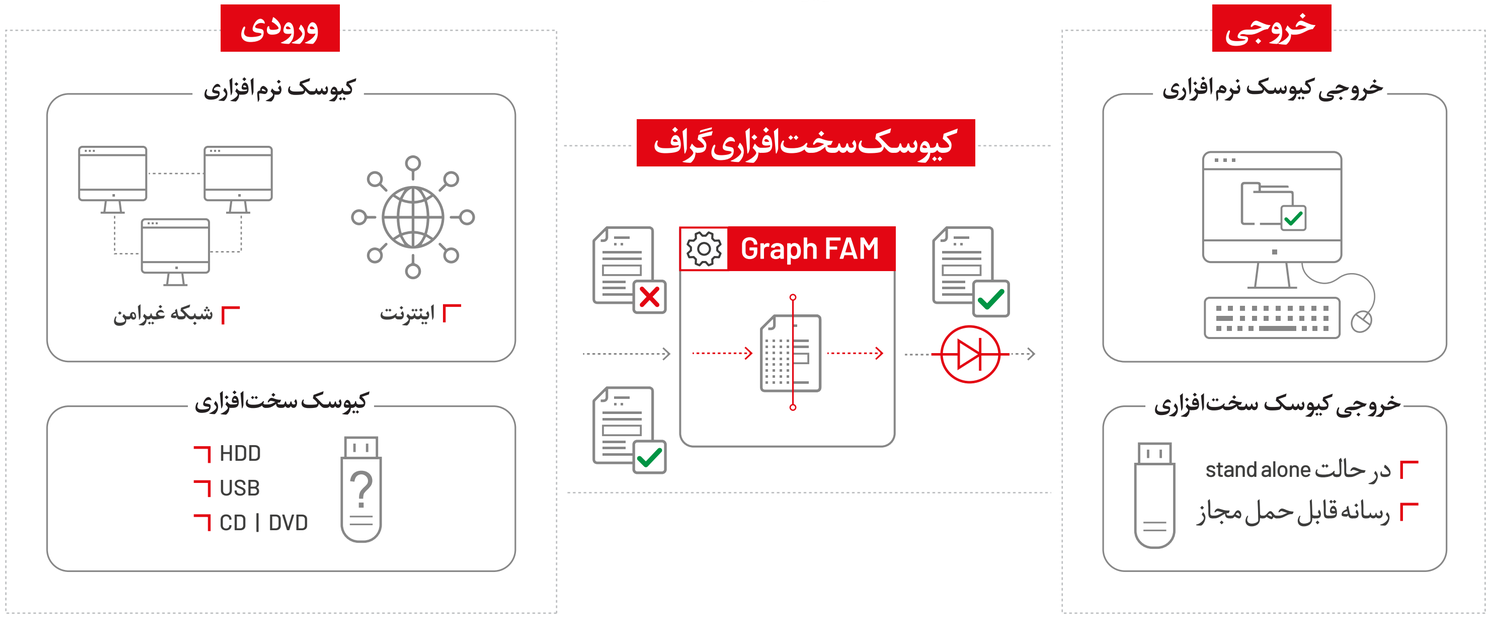
ماژول تحلیل فایل گراف (Graph FAM) به سازمان‌ها کمک می‌کند تا فایل‌های مخربی را که وارد شبکه می‌شوند شناسایی و مسدود کنند. این فایل‌ها یا توسط عامل انسانی (Actor Type: Human) مانند ارباب رجوع و رسانه‌های قابل حمل کارکنان وارد شبکه سازمان می‌شوند و یا از طریق عامل سیستمی (Actor Type: System) مانند ایمیل‌ها، نرم‌افزارهایی که دسترسی انتقال فایل در شبکه دارند مثل انواع اتوماسیون اداری، پرتال‌های سازمانی.

سامانه تحلیل فایل گراف ورودی‌های مختلفی بر اساس مدل‌های پیاده‌سازی متنوع خود دارد. در مرحله تحلیل، فایل‌ها براساس مراحل ذکر شده در تصویر شماره ۱ بررسی می‌شوند و موارد مجاز از طریق خروجی‌های استاندارد شده در مدل‌های سخت‌افزاری و نرم‌افزاری برای استفاده در اختیار کاربران قرار می‌گیرند.



تصویر شماره ۴

تصویر شماره ۵



شرکت دانش‌بنیان گراف | تهران، شهرک سئول، دوم شرقی، شماره۴ | ۶۰۰۰ ۴۷۷۱ ۰۲۱

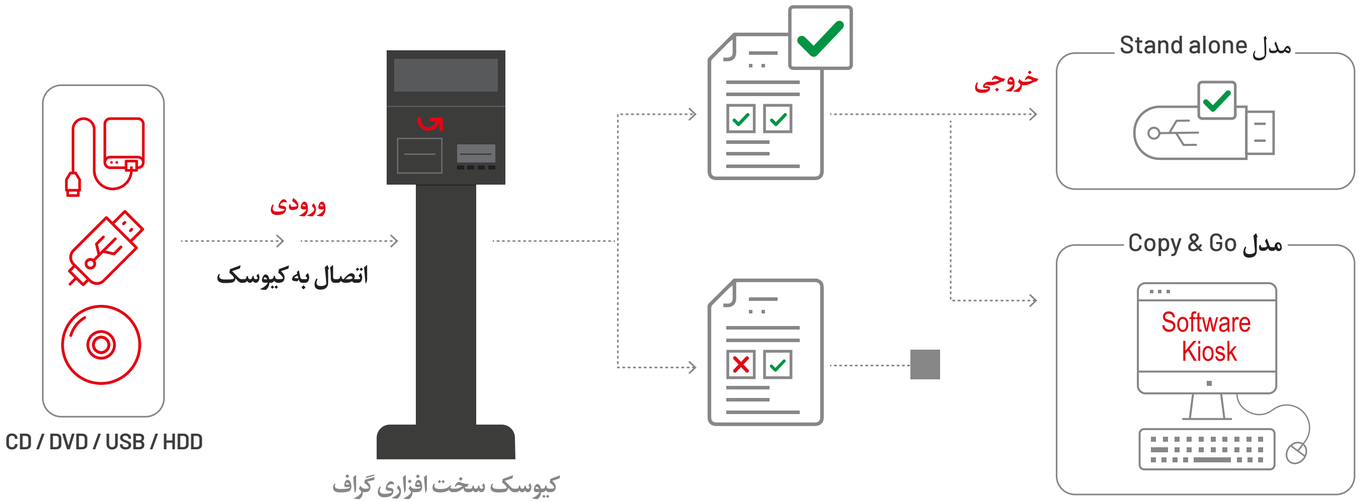
کیوسک سخت‌افزاری گراف

سامانه کیوسک گراف با استفاده از ماژول تحلیل فایل، بستر مطمئنی برای انتقال امن فایل در شبکه‌های عمومی و ایزوله تا سطح (Air-gaped Network) را برای سازمان‌ها فراهم می‌کند. سامانه کیوسک گراف در مدل‌های سخت افزاری (ایستاده/ رومیزی/ دیواری) و نرم‌افزاری ارائه می‌شود و هدف آن انتقال فایل از شبکه‌ی عمومی/اینترنت به شبکه‌ی خصوصی/ایزوله است. در این سامانه،کاربر برای انتقال فایل به شبکه‌ی خصوصی/ایزوله، از یکی از تجهیزات هارد اکسترنال، فلش و CD/DVD استفاده می‌کند.

در مدل سخت‌افزاری کیوسک با اتصال یکی از تجهیزات بالا به دستگاه ، فایل‌های کاربر بررسی می‌شود. در این مرحله کیوسک، پس از بررسی فایل‌ها از نظر امنیتی، در صورت نبود مشکل، فایل‌ها را به صورت مستقیم و یا با استفاده از یک دستگاه یکسو کننده داده در مقصد کپی می‌کند.

مزایای کیوسک گراف

- نصب سریع
- آپدیت آسان (به دو شیوه آفلاین و آنلاین)
- کاربری ساده



تصویر شماره ۶

مدل‌های ارائه آنتی ویروس‌ها در سامانه تحلیل فایل گراف

پنج آنتی‌ویروس: Windows Defender، ClamAV، AVIRA، McAfee، AhnLab

ده آنتی‌ویروس: Bitdefender، eset، KASPERSKY، SOPHOS، EMSISOFT

دستگاه کیوسک که در ورودی بخش‌های حساس سازمان قرار می‌گیرد، به دو مدل مستقل (Stand Alone) SA و (Copy & Go) C&G قابل پیاده‌سازی است. در مدل مستقل SA پردازش‌ها در داخل کیوسک به صورت محل انجام می‌شود و بعد از اتمام فرایند، فایل‌های امن را به کاربر تحویل می‌دهد. در مدل (Copy) C&G & Go دستگاه کیوسک فایل‌ها را دریافت می‌کند و به کاربر رسید تحویل می‌دهد. در این مدل کاربر نیاز نیست تا اتمام پردازش منتظر بماند.

	مدل مستقل (Stand Alone) SA	مدل (Copy & Go) C&G
ظرفیت انتقال فایل	۱۰ هزار فایل	نامحدود
ظرفیت انتقال حجم فایل	۱۰۰ گیگ	نامحدود
وضعیت کاربر	نیاز به انتظار تا پایان پردازش	تحویل فایل و دریافت فوری رسید
موتور پردازشی	Graph FAM	Graph FAM
نحوه مدیریت کاربران	تعریف تک به تک و دستی	یکپارچه و از طریق FMS
شرایط بروزرسانی	بروز رسانی تک به تک و دستی	نرم‌افزاری، یکپارچه و ارزان
شرایط مدیریت شبکه	بدون نیاز به اتصال دائمی به شبکه	نیاز به ارتباط شبکه کامل و پایدار

کیوسک سخت‌افزاری گراف در سه شکل فیزیکی **دیواری**، **رومیزی** و **ایستاده** قابل ارائه است:

کیوسک ایستاده

کیوسک رومیزی

کیوسک دیواری

شرکت دانش‌بنیان گراف | تهران، شهرک سئول، دوم شرقی، شماره۴ | ۶۰۰۰ ۴۷۷۱ ۰۲۱

ساماندهی ورود انواع فایل به سازمان

در بسیاری از سازمان‌ها مراجعان و ارباب رجوع برای مقاصد گوناگون، فایل‌های مختلفی به سازمان وارد می‌کند. این فایل‌ها که روی بر روی انواع رسانه‌های قابل حمل به سازمان وارد می‌شوند می‌توانند حاوی انواع بدافزار و فایل مخرب باشند.
کیوسک سخت‌افزاری بدون اتصال کاربر به شبکه داخلی ورود انواع فایل را به سازمان ساماندهی می‌کند و امکان آلوده‌سازی از این شیوه را به حداقل می‌رساند.

پشتیبانی از انواع رسانه‌های قابل حمل

محصولات سخت‌افزاری کیوسک، از رایج ترین انواع رسانه های قابل حمل، از جمله درایوهای فلاپی، با انواع رسانه خوان‌های داخلی درجلوی کیوسک پشتیبانی می‌کنند.

امکان نصب آسان

هر دستگاه کیوسک گراف در زمان استقرار با یک سیستم عامل، نرم‌افزار تحلیل فایل گراف از پیش نصب شده، اترنت و لوازم جانبی نصب، ارائه می‌شود.

طراحی کاربرپسند و کاربری آسان توسط ارباب رجوع

رابط کاربری برنامه که توسط کاربر نهایی و ارباب رجوع استفاده می‌شود، طراحی کاربرپسندی دارد که افراد به سادگی و بدون نیاز به آموزش قبلی قادر هستند فرایند اتصال رسانه قابل حمل و پردازش فایل‌های موجود در انرا دنبال کنند.

شرکت دانش‌بنیان گراف | تهران، شهرک سئول، دوم شرقی، شماره۴ | ۶۰۰۰ ۴۷۷۱ ۰۲۱

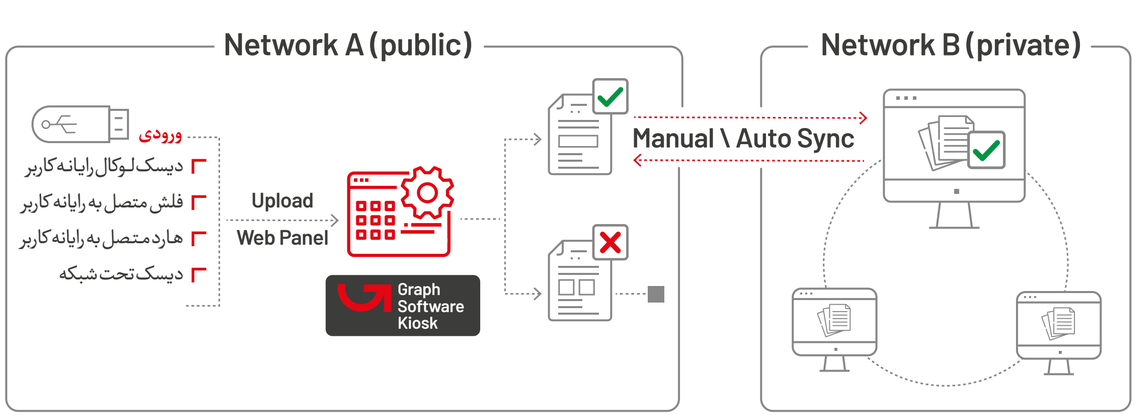
مشخصات فنی مدل سخت افزاری کیوسک گراف

ویژگی ها	کیوسک گراف
انواع رسانه قابل پشتیبانی	4x USB 3.0 Type A 2x USB 2.0 Type A CD/DVD Player
نمایشگر	Display type: VA 19” Screen Size 60Hz Refresh Rate Resolution 1368 x 768 Aspect Ratio: 16:9
چاپگر	Print width: 56mm (max) Paper load: front 150 lines/sec Paper width: 48/56/58/60
شیوه‌های ارتباطی	Ethernet with exterior RJ45 port

شرکت دانش‌بنیان گراف | تهران، شهرک سئول، دوم شرقی، شماره۴ | ۶۰۰۰ ۴۷۷۱ ۰۲۱

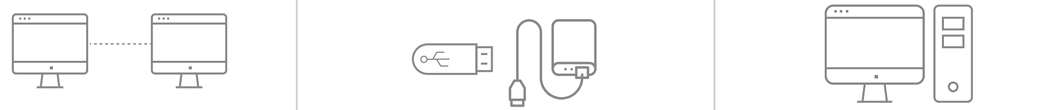
محصولات نرم‌افزاری کیوسک گراف

سامانه کیوسک نرم‌افزاری گراف به هدف انتقال فایل از شبکه‌ی عمومی/اینترنت به شبکه خصوصی/ایزوله و یا بالعکس طراحی شده است. این سامانه براساس زیرساخت ابری پیاده‌سازی شده که به صورت ابر خصوصی (private cloud) در داخل سازمان راه‌اندازی می‌شود. در این سامانه، کاربر برای انتقال فایل از شبکه عمومی به شبکه‌ی خصوصی/ایزوله یا بالعکس، وارد پنل کاربری تحت وب خود شده و فایل را آپلود می‌کند.



▲ تصویر شماره ۷

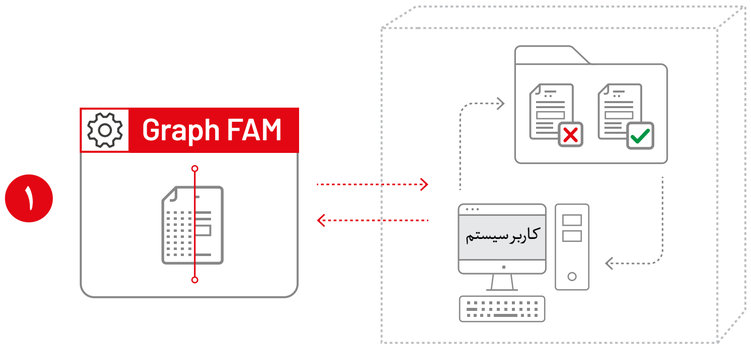
آپلود فایل می‌تواند از یکی از منابع زیر باشد



با انتخاب فایل از یکی از مبادی بالا، فایل‌ها آپلود شده و پس از بررسی فایل‌ها از نظر امنیتی، در صورت نبود مشکل، فایل‌ها به صورت مستقیم و یا با استفاده از یک دستگاه یکسو کننده داده به مقصد کپی می‌شود. انتقال می‌تواند یکی از ۴ این وضعیت باشد:

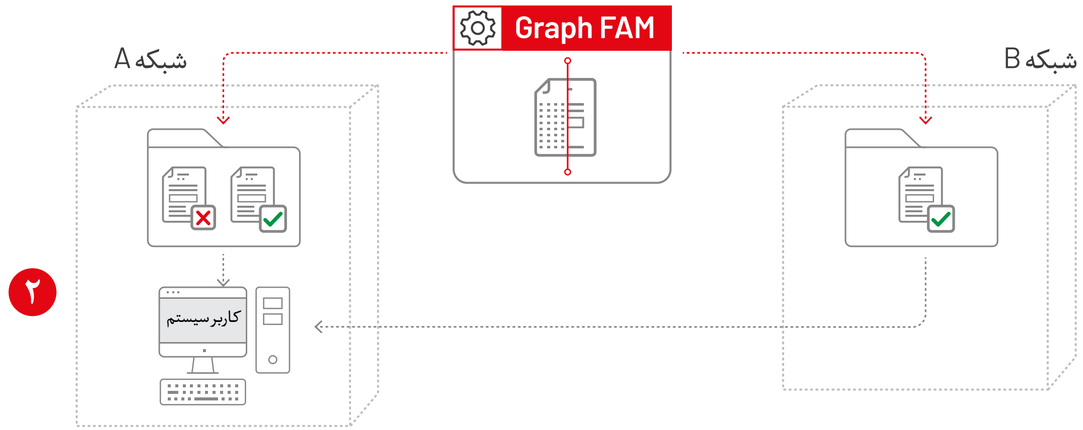
ذخیره فایل در پنل کاربر آپلود کننده در شبکه جاری

در این حالت فایل پس از پردازش در صورت مجاز بودن، در فضای ابری مربوط به کاربر آپلود کننده ذخیره شده و کاربر می‌تواند در دفعات بعدی فایل را دانلود کرده و یا به شبکه‌ها و کاربرهای دیگر منتقل کند.



شبکه A

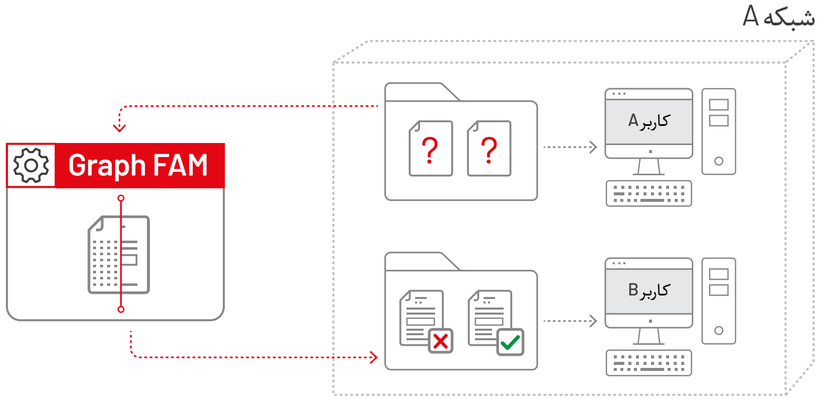
شرکت دانش‌بنیان گراف | تهران، شهرک سئول، دوم شرقی، شماره۴ | ۶۰۰۰ ۴۷۷۱ ۰۲۱



۲

انتقال فایل به پنل کاربر آپلودکننده در شبکه دیگر (از ایزوله به اینترنت و از اینترنت به ایزوله)

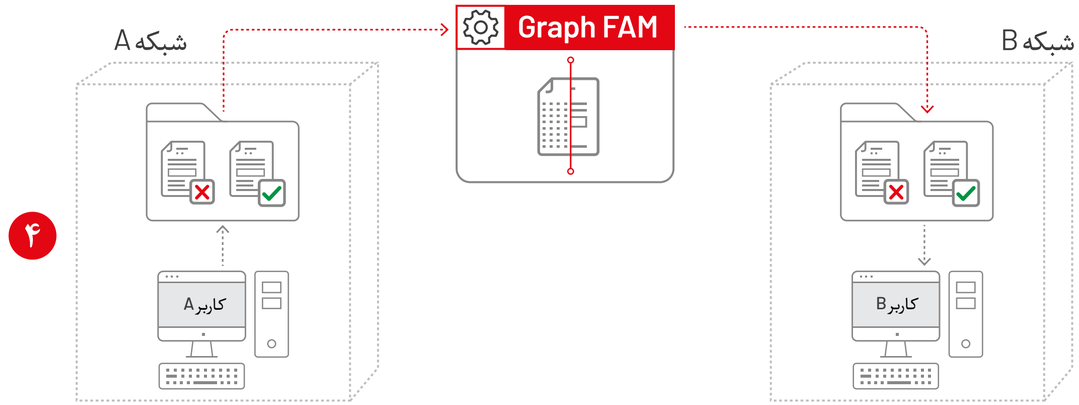
در این حالت فایل پس از پردازش در صورت مجاز بودن، در فضای ابری کاربر آپلود کننده در شبکه دیگر ذخیره می‌شود. به عنوان مثال کاربر A فایلی را از اینترنت دانلود کرده و پس از آپلود و بررسی پاک بودن فایل، آن را در پنل خود در شبکه ایزوله غیر اینترنت دریافت می‌کند.



۳

انتقال فایل به پنل کاربر دیگر در شبکه جاری

در این حالت فایل پس از پردازش در صورت مجاز بودن، به پنل کاربر دیگری که مشخص شده در همان شبکه منتقل می‌شود. به عنوان مثال کاربر A در شبکه ایزوله فایل گزارش خود را برای کاربر B در همان شبکه ایزوله ارسال کرده و کاربر دوم در پنل خود فایل را دریافت می‌کند.



۴

انتقال فایل به پنل کاربر دیگر در شبکه دیگر (از ایزوله به اینترنت و از اینترنت به ایزوله)

در این حالت فایل پس از پردازش در صورت مجاز بودن، در فضای ابری کاربر دیگری در شبکه دیگر ذخیره می‌شود. به عنوان مثال کاربر A فایلی را از اینترنت دانلود کرده و پس از آپلود و بررسی پاک بودن فایل، کاربر B آن را در پنل خود در شبکه ایزوله غیر اینترنت دریافت می‌کند. این سناریو برای انتقال از شبکه ایزوله به شبکه اینترنت نیز امکان‌پذیر است.

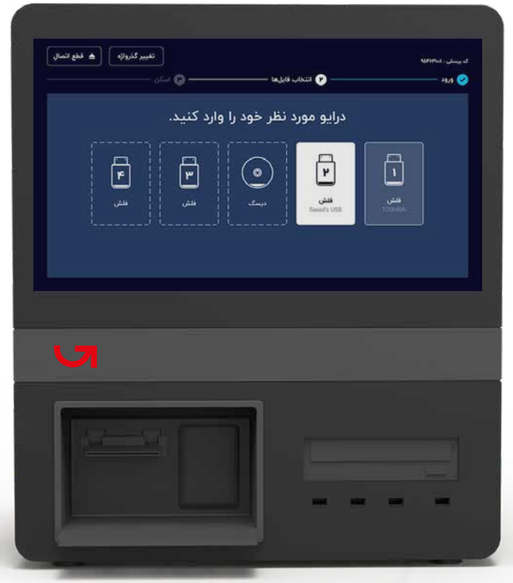
شرکت دانش‌بنیان گراف | تهران، شهرک سئول، دوم شرقی، شماره۴ | ۶۰۰۰ ۴۷۷۱ ۰۲۱

سامانه کیوسک مبتنی بر Agent گراف

سامانه کیوسک مبتنی بر Agent گراف به هدف انتقال فایل از شبکه عمومی/اینترنت به شبکه خصوصی/ایزوله و یا بالعکس براساس دستگاه‌های ذخیره داده قابل حمل طراحی شده است. این سامانه براساس زیرساخت ابری است که به صورت ابر خصوصی (private cloud) در داخل سازمان راه‌اندازی می‌شود.

در این سامانه، کاربر برای انتقال فایل از شبکه عمومی به شبکه خصوصی/ایزوله یا بالعکس، از فلش/هارد اکسترنال استفاده می‌کند.

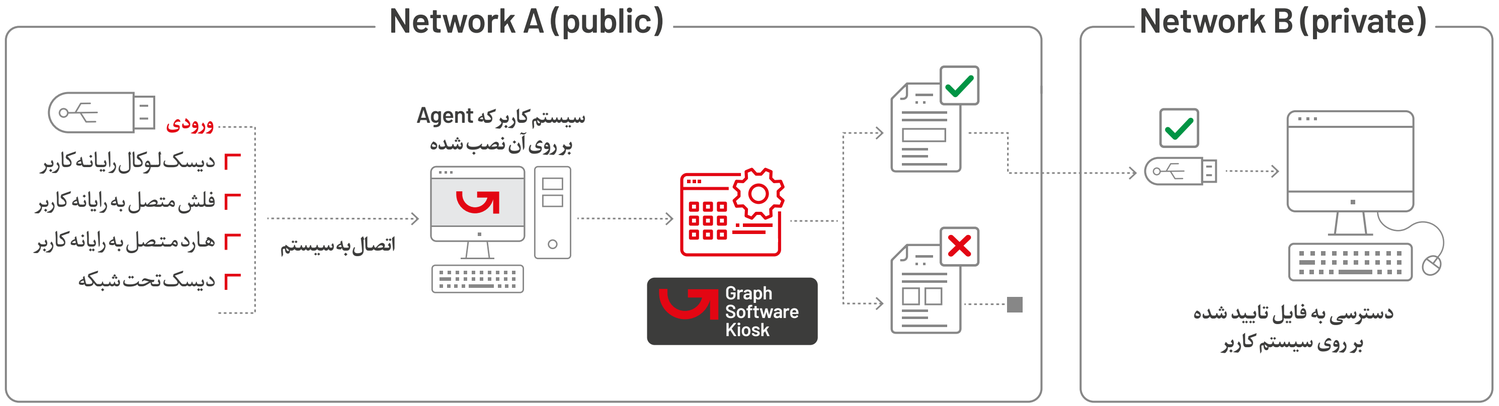
کاربر دستگاه ذخیره‌ساز قابل حمل خود را به کامپیوتر خود در شبکه اینترنت/عمومی یا ایزوله/خصوصی متصل می‌کند. Agent بر روی کلیه سیستم‌ها نصب شده و قابلیت device control را دارد. در این حالت فلش پس از وصل شدن، امکان باز شدن و کپی فایل از/به آن وجود ندارد.



Agent نصب شده به صورت خودکار اتصال فلش را شناسایی کرده، فایل‌ها را برای انجین پردازشی که به صورت ابر خصوصی در شبکه سازمان قرار دارد، ارسال می‌کند. فایل‌ها پس از پردازش و تطبیق با قوانین و چارچوب‌های سازمان از نظر آلودگی بررسی شده و در صورت عدم وجود آلودگی، به Agent گزارش داده می‌شوند.

Agent اجازه read (خواندن) را بر روی فلش برای فایل‌های مجاز اعلامی فعال می‌کند. به این ترتیب کاربر می‌تواند فایل‌ها را از دستگاه ذخیره ساز قابل حمل بر روی pc خود کپی نماید.

همچنین کاربر برای انتقال فایل به کاربر دیگر یا شبکه دیگر می‌تواند از طریق دستگاه ذخیره ساز قابل حمل (به عنوان مثال فلش) و یا از طریق پنل وب کیوسک نرم‌افزاری اقدام کند.



تصویر شماره ۸

شرکت دانش‌بنیان گراف | تهران، شهرک سئول، دوم شرقی، شماره۴ | ۶۰۰۰ ۴۷۷۱ ۰۲۱

بسته‌های پیشنهادی محصولات کیوسک گراف

مشخصات	بسته استاندارد	بسته حرفه‌ای	بسته ویژه
شکل فیزیکی کیوسک سخت‌افزاری	ایستاده | دیواری | رومیزی	ایستاده | دیواری | رومیزی	ایستاده | دیواری | رومیزی
نوع نسخه Graph FAM	فقط اتصال دستگاه سخت‌افزاری کیوسک	فقط اتصال دستگاه سخت‌افزاری کیوسک	اتصال به نسخه‌های نرم‌افزاری کیوسک
موتورهای آنتی ویروس	۵ آنتی ویروس شامل Emsisoft, ClamAV, Avira, McAfee, AhnLab	۱۰ آنتی ویروس شامل AhnLab, Eset, Avira, Kaspersky, Sophos, Bitdefender, Microsoft, ClamAV, McAfee, Emsisoft	۱۰ آنتی ویروس شامل AhnLab, Eset, Avira, Kaspersky, Sophos, Bitdefender, Microsoft, ClamAV, McAfee, Emsisoft
بررسی فایل با دیتابیس فایل‌های پاک (Benign list)	✓	✓	✓
بررسی فایل با دیتابیس فایل‌های آلوده شناخته‌شده توسط ماژول تحلیل فایل گراف	✓	✓	✓
پشتیبانی از نوع کاربر سوم به جز کاربر معمولی و مدیر سامانه	✗	✓	✓
موتور پردازشی YARA با قوانین اختصاصی شرکت گراف	✗	✓	✓
بررسی فایل با ماژول هوش تهدید Threat Intelligence	✗	✗	✓
ماژول sandbox	✗	✗	✓

GRAPH

شرکت دانش‌بنیان گراف

| تهران، شهرک سئول، دوم شرقی، شماره۴ |

۰۲۱ ۴۷۷۱ ۶۰۰۰

www.graph-inc.ir