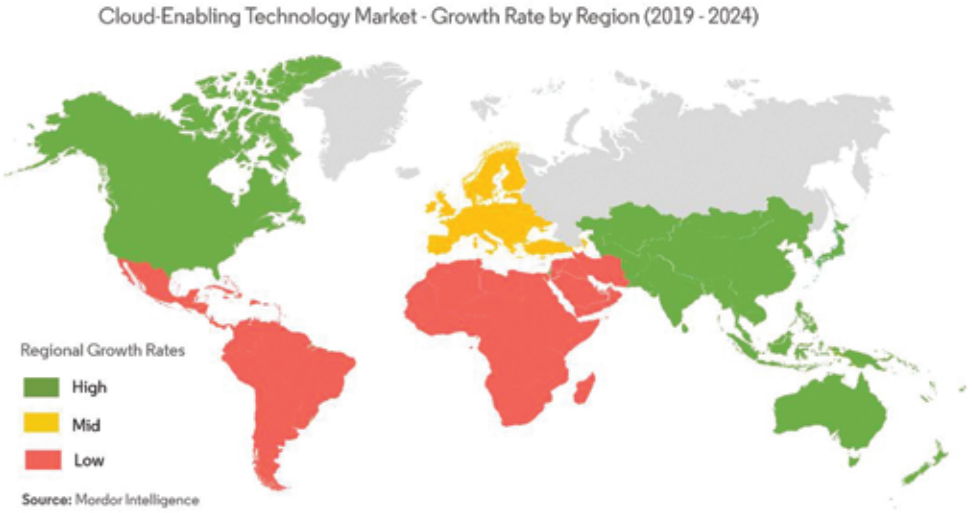

پلتفرم ابریکم
abricam
www.abricam.ir

رایانش ابری

رایانش ابری (Cloud Computing) مفهومی در حوزه فن‌آوری اطلاعات و ارتباطات است که در آن منابع محاسباتی و ذخیره‌سازی براساس نیاز و مجوزها در حوزه‌های مشخص جغرافیایی و سازمانی در اختیار کاربران قرار می‌گیرد. این مفهوم بر پایه و فلسفه به حداکثر رساندن راندمان، توسعه‌پذیری، امنیت و کاهش هزینه‌ها استوار است. استفاده حداکثری از ظرفیت‌های موجود، کاهش هزینه‌ها، امنیت بالا، کیفیت مناسب، توسعه سریع و عدم وابستگی به شرایط محیطی از دلایل اصلی و شتابان استفاده از رایانش ابری در جهان است. خوشبختانه در کشور عزیزمان ایران نیز رایانش ابری در حال توسعه و استفاده است.



استفاده از فناوری‌های نوین و جایگزین نیاز به شناخت، برنامه‌ریزی و سرمایه‌گذاری دارد. تعیین الویت و توجه به زمان از عوامل مهم در پیشرفت و بکارگیری فناوری‌های کاربردی هستند.

رایانش ابری بستر فن‌آوری‌های نوین و موتور محرک پلتفرم‌ها و ساختارهای منعطف، چابک و مقیاس پذیر است و بیش از ۹۳٪ کسب و کارهایی که از رایانش ابری استفاده می‌کنند معتقدند که استفاده از سرویس‌های ابری، علاوه بر کارآیی و صرفه‌جویی، امنیت سایبری آنها را نیز بالا برده است. پیش‌بینی می‌شود که تا پایان سال ۲۰۲۵ میلادی بیش از ۸۰٪ درصد عملیات سازمان‌ها در بخش‌های خصوصی، عمومی و دولتی بر بستر ابری قرار گیرند.

پایش تصویر ابری

در چند دهه‌ی اخیر هماهنگ با پیشرفت علوم و فنون، شاهد تغییرات بی‌شماری در فناوری و نحوه استفاده از دوربین‌های مداربسته بوده‌ایم. این تحول از تجهیزات آنالوگ و ذخیره‌سازی بر روی نوارهای مغناطیسی شروع شده و در دو دهه گذشته با استفاده وسیع از تجهیزات و دوربین‌های دیجیتال و نرم‌افزارهای متنوع رو به رشد بوده است. هم اکنون با بهبود روش‌های انتقال تصاویر و طراحی نرم‌افزارها، استفاده از مفاهیم رایانش ابری در این حوزه تخصصی و پیچیده نیز مورد استفاده قرار گرفته است.

پایش تصویر ابری(Video Surveillance as a Service (VSaaS یا بعبارتی Cloud VMS در برگیرنده مفهوم و ساختار رایانش ابری برای کاربردهای پایش تصویر در دوربین‌های مداربسته است

در بسیاری کشورها در حوزه‌های گوناگون اعم از امنیت خانگی، کسب و کارهای کوچک و متوسط، شرکت‌های بزرگ و چند ملیتی، بانک‌ها، موسسات مالی، بیمه، شهر هوشمند، امنیت شهری، امنیت مراکز انرژی، امنیت مراکز نظامی، حساس و حیاتی و حتی مرزها استفاده از پایش تصویر ابری در حال پیشرفت و توسعه است.

پیش‌بینی شده که بکارگیری نرم افزارها و تجهیزات مدیریت و پایش تصاویر اعم از VMS و NVR تا سال ۲۰۳۰ میلادی، در اکثر موارد با "پایش تصویر ابری" جایگزین خواهند شد.

VSaaS

VMS

NVR/DVR

حجم بازار پایش تصویر ابری در سال ۲۰۱۸ میلادی ۱۸/۵ میلیارد دلار بوده که تا سال ۲۰۲۶ میلادی به حداقل ۵۲/۹ میلیارد دلار خواهد رسید!

اولین دوربین مداربسته در سال ۱۹۴۲ میلادی توسط مهندسین آلمانی برای مشاهده عملکرد لانچر موشک V۲ مورد استفاده قرار گرفته است.

امنیت سایبری

بـازار دوربین‌هـای مـدار بسـته بسـیار رقابتـی و قیمـت یـک پارامتـر مهـم و تعییـن کننـده اسـت. بسـیاری از سـازندگان بـرای پاییـن نگـه داشـتن قیمـت، نسـبت بـه کاهـش و حـذف مـواردی کـه بـه سـادگی توسـط مشـتریان قابـل شناسـایی نیسـتند اقـدام می‌کننـد کـه از آن جملـه می‌تـوان بـه امنیـت سـایبری اشـاره کـرد. اسـتفاده از اِلمان‌هـای الکترونیکـی نامرغـوب و بکارگیـری روش‌هـای غیـر اصولـی تولیـد سـبب شـده تـا شـاهد رشـد قـارچ گونـه انـواع برندهـای ناشـناخته باشـیم. بخشـی از چالش‌هـا و مشـکلات امنیـت سـایبری در دوربین‌هـای مداربسته را در جدول زیر می‌توان مشاهده کرد:

سازندگان و پیمانکاران	کاربران
وابستگی‌های سیاسی و امنیتی به دلایل مالی و نفوذ	خطای انسانی به عمد یا سهو و مباحث فساد و نفوذ
استفاده از برندهای OEM با جزییات و منابع نامشخص	عدم بروزرسانی رمزهای عبور و نرم‌افزارهای دوربین و پایش
حذف منابع و عدم انجام تست امنیت برای کاهش هزینه‌ها	عدم توجه به امنیت سایبری، ارتباطی و سیستم‌عامل‌ها
احتمال وجود حفره امنیتی عمدی یا سهوی در منابع	نیاز و لزوم مشاهده تصاویر از راه دور بدون توجه به خطرات
عدم رفع نقص‌ها حتی بعد از اعلام برای کاهش هزینه‌ها	استفاده از نرم‌افزارهای نامطمین و کِرَک شده!
عدم توجه کافی به سازگاری و مطابقت منابع و تجهیزات	عدم توجه به آموزش و یادگیری و بروز شدن
احتیاط در ارایه توصیه‌های فنی برای حفظ مشتری	خیال راحت با تصور شبکه مجزا و مستقل داشتن!
عدم سرمایه‌گذاری در آموزش و تکنولوژی‌های نوین	عدم ارزیابی مناسب کیفی و توجه بیش از اندازه به قیمت

براسـاس نظـر سـنجی مشـترک شـرکت‌های معتبـر Axis و Genetec فقـط ۱۵٪ از سـازمان‌ها آمادگـی کافـی بـرای کاهـش یـا مقابلـه بـا یـک تهدیـد سـایبری در شـبکه دوربین مداربسته خود را دارا هستند.

تهدیدات سایبری شبکه

در سپتامبر و اکتبر ۲۰۱۶ بزرگترین حملات سایبری به چند صد هزار دوربین، VMS، NVR، DVR در امریکای شمالی انجام شده است. براساس گزارش‌ها و اطلاعات اعلام شده بیش از یک میلیون دوربین در این حملات سایبری آلوده شدند و این در حالی بود که اکثر دارندگان دوربین‌ها از آلودگی آنها اطلاعی نداشتند!

در جولای ۲۰۱۷ میلادی، محققان امنیت سایبری یک نقص جدی در استاندارد معروف ONVIF پیدا کرده و آن را "پیچک شیطان" (Devil's Ivy) نامیدند. این نقص به هکرها اجازه می‌دهد تا کنترل دوربین‌های سازگار با ONVIF را به طور کامل در دست بگیرند. بیشتر انواع دوربین‌ها حتی با برندهای معروف و کیفیت بالا در این خصوص آسیب‌پذیر هستند. متاسفانه در خصوص رفع این نقیصه توسط سازندگان دوربین‌ها هیچ توضیح و اطلاعاتی ارایه نشده است.

داشتن محیط‌های کاری پویا و توزیع شده با انعطاف پذیری مناسب نیاز امروز برای افزایش کارایی و سرعت عمل است. این موضوع به معنای افزایش ارتباط و اتصال منابع و ساختارها و در نتیجه ایجاد شرایط ناامن است که سبب افزایش حملات سایبری در جهان نیز شده است. عدم توجه و سرمایه‌گذاری کافی و به موقع در امنیت سایبری سبب بروز چالش ها و خسارات جبران‌ناپذیری می‌شود. خوشبختانه اجرای مرحله‌ای همراه با الویت‌بندی این مهم میسر است و می‌توان براساس شرایط و امکانات هر مجموعه‌ای نسبت به طراحی و تعریف مراحل اجرا اقدام نمود، لذا مهمترین قدم گرفتن تصمیم است !

شناخت، تداوم، ارتقا و بهبود شرایط امنیت سایبری، علاوه بر ایجاد اطمینان در استفاده موثر از امکانات، سبب کاهش ریسک و صرفه‌جویی اقتصادی زیادی نیز خواهد شد.

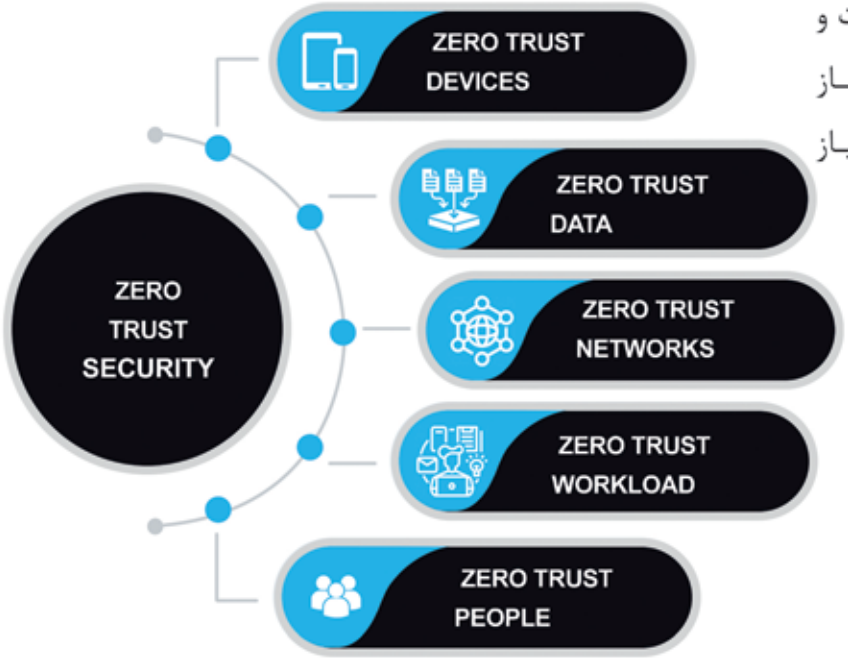
دوربین‌های مدار بسته به دلیل داشتن ماهیت تصویری مورد علاقه و توجه مهاجمین و دولت‌های متخاصم هستند. اینگونه حملات توسط طرفین کمتر افشا می‌شوند! می‌دانید چرا؟

اعتماد صفر

اگـر بخواهیـم امنیـت سـایبری مناسـبی داشـته باشـیم، ابتـدا بایـد یـک دیـدگاه و شـیوه کارآمـد را برگزینیـم. یکـی از معتبرتریـن ایـن شـیوه‌ها "اعتمـاد صفـر" (Zero Trust) اسـت کـه اولیـن بـار توسـط اسـتفان مـارش در سـال ۱۹۹۴ میـلادی مطـرح شـد. بـه مـرور ایـن مفهـوم توسـعه و تکامـل یافـت و امـروزه بطـور وسـیعی در طراحـی سـاختارهای مربـوط بـه امنیـت سـایبری مـورد اسـتفاده قـرار می‌گیـرد. فلسـفه وجـود یـک سـاختار بـر مبنـای اعتمـاد صفـر بـر دو اصـل زیـر استوار است :

اصـل اول: مهاجمـان سـایبری در داخـل و خـارج از سـاختار هـر سـازمانی وجـود دارنـد، بنابرایـن بـه هیـچ کاربـر یـا دسـتگاهی یـا نرم‌افـزاری نبایـد بـه طـور کامـل اعتمـاد کـرد. نرم‌افزارهـای غیـر اصـل و کـرک شـده دارای ضعـف امنیتـی بیشتری هستند و باید از چرخه کاری و استفاده حذف شوند.

اصـل دوم: دسـتیابی نرم‌افزارهـا، تجهیـزات و کاربـران بایـد در حداقـل دسترسـی مـورد نیـاز باشـد. یعنـی بـه آنهـا فقـط بـه انـدازه‌ای کـه نیـاز کاری دارند دسترسی داده شود.



بـه چـه میـزان از عـدم دسترسـی افـراد غیرمجـاز بـه تصاویـر دوربیـن هـای مداربسـته در سـازمان خـود مطمئن هستید؟

تروجان، ویروس، جاسوس‌افزار و حفره امنیتی

آلودگی تجهیزات و نرم‌افزارها به تروجان، ویروس، جاسوس‌افزار و حفره‌های امنیتی از پیش نصب و تعبیه شده، موضوعی متداول و غیر قابل انکاری است و براساس اهداف و ماهیت مهاجمان سایبری جنبه امنیتی یا اقتصادی دارد. در این وضعیت از بین بردن اطلاعات، تغییر نامحسوس شرایط و تنظیمات، انجام عملیات و امور خاص در شرایط و زمان‌های مورد نظر و بسیاری موارد دیگر براساس هدف و ماهیت مهاجمین قابل انجام است.

شواهد بسیاری از وجود حفره‌های امنیتی که بطور عمد توسط سازندگان به دلایل مختلف در دوربین‌ها، تجهیزات شبکه، نرم‌افزارهای کرک شده و قفل شکسته و تجهیزات ضبط تصاویر تعبیه می شوند وجود دارد.

نرم افزارهای کِرَک شده و قفل شکسته، عدم بروزرسانی نرم‌افزارها و سیستم‌عامل‌ها، دوربین‌های مشکوک و توهم شبکه اختصاصی از عوامل اصلی در افزایش تهدیدات و حملات سایبری هستند.

عدم توجه به اصول اخلاقی و منافع و امنیت ملی در بکارگیری نرم‌افزارهای کرک شده و قفل شکسته تبدیل به یک فرهنگ کاری بخصوص در سازمان‌های دولتی و حکومتی شده است. این معضل، انگیزه جوانان و کارشناسان و سرمایه‌گذاری در این حوزه را به شدت کاهش داده است!

چالش‌های پایش تصویر

در حال حاضر چالش‌های بسیاری در استفاده از دوربین‌های مداربسته براساس تجهیزات محلی گریبانگیر استفاده‌کنندگان در رده‌های مختلف کاربری است که مهمترین آنها به شرح زیر هستند:

۱- تخریب و سرقت: بروز عوامل مختلف نظیر آتش سوزی، تخریب و سرقت تجهیزات ضبط محلی از مواردی است که در روش‌های سنتی و متداول دوربین‌های مداربسته سبب از بین رفتن کلیه اطلاعات و تصاویر ضبط شده می‌شوند.

۲- نگهداری و تعمیرات: وجود یک ساختار مناسب پشتیبانی و نگهداری سبب کاهش بروز مشکلات نرم‌افزاری، سخت‌افزاری، شبکه و پشتیبان‌گیری می‌شود. بسیاری از سازمان‌ها به دلیل وسعت جغرافیایی و هزینه‌های بالا، امکان ایجاد یک نظام پشتیبانی فنی را ندارند که می‌تواند صدمات جبران‌ناپذیری را بوجود آورد.

۳- اعلام خطر: محدود بودن امکانات نرم‌افزاری و ارتباطی در قبال اتصال به تجهیزات ضبط تصاویر محلی سبب می‌شود تا استفاده از مکانیزم‌های اعلام خطر به افراد و سیستم‌های مرتبط، به موقع، سریع و مناسب نباشند.

۴- دسترسی و نظارت: بسیاری از سازمان‌ها و مجموعه‌ها دارای دفاتر و شعب متعدد در سطح کشور هستند و بروزرسانی نرم‌افزارها، تغییر سطح دسترسی کاربران، تهیه پشتیبان، نظارت بر روند امور و بسیاری موارد فنی و مدیریتی در عمل غیرممکن و گران هستند.

۵- تجمیع تصاویر: تنوع محصولات سخت‌افزاری و نرم‌افزاری سبب شده تا یکی از معضلات بخصوص در سازمان‌های بزرگ و توزیع شده امکان تجمیع و دسترسی به تصاویر دوربین‌های نصب شده در سطح کشور باشد.

آیا می دانید که یکی از خدمات شرکت پردازش تصویر کمان طراحی و پیاده‌سازی ساختار با اعتماد صفر در حوزه مدیریت، پایش، نظارت و آنالیز تصاویر است؟

با توجه به مشکلات و چالش‌های بسیاری که امروزه در استفاده از تجهیزات و نرم‌افزارها به صورت محلی با آنها روبرو هستیم، استفاده از پایش تصویر ابری می‌تواند نقش مفید و مهمی در افزایش امنیت و کاهش هزینه‌ها ایفا نماید.

۶- اتصال به سایر نرم‌افزارها: محدودیت‌های بسیاری در نرم‌افزارها و تجهیزات متنوع موجود برای اتصال به سایر سیستم‌ها وجود دارد. حتی در صورت اتصال نرم‌افزاری، هزینه سنگینی از لحاظ تعدد سایت‌ها، تجهیزات، لایسنس و پشتیبانی را باید تقبل نمود.

۷- امنیت سایبری: تعدد سرورها و مراکز ذخیره‌سازی آن هم در نقاط و مکان‌های مختلف به معنای اجرای کامل ساختار امنیت برای هر سایت است. این مهم علاوه بر نیاز به تجهیزات و نرم افزارهای پیچیده، نیاز به حضور دایم کارشناسان خبره در همه سایت‌ها را به دنبال دارد که در عمل چندان امکان‌پذیر نیست.

۸- اصالت نرم‌افزار: اطمینان از عدم وجود حفره امنیتی در نرم افزارهای مورد استفاده یکی از مهمترین چالش‌های موجود در کشور است. شرایط خاص و حساس امنیت فیزیکی در کنار عدم توجه به اصالت محصولات به دلایل هزینه و یا نفوذ سبب شده تا ریسک بالایی در استفاده از محصولات پایش تصویر را شاهد باشیم.

۹- هزینه بالا: هر تصمیمی که در امور مدیریتی و کارشناسی بدون توجه به ریسک‌های امنیتی صورت می‌گیرد، می‌تواند به یک فاجعه تبدیل شود. استفاده از روش‌های نوین و ابزار مناسب الزامی است.

آیا وجود حفره‌های امنیتی در دوربین‌ها، تجهیزات و نرم‌افزارهای بدون تاییدیه از مراجع ذیصلاح کشور را جدی می دانید؟

آیا داشتن تاییدیه های فنی و امنیتی از مراجع ذیصلاح در انتخاب نرم‌افزارها اهمیت دارد؟

چرا مراجع مهم و کلیدی در سطح بالای کشور داشتن تاییدیه‌هایی فنی و امنیتی را الزامی کرده‌اند؟

پایش تصویر در جهان

امروزه کاربرد دوربین‌های مداربسته نیاز به توجیه و تفصیل ندارد و می‌دانیم که بدون این تجهیزات نظارت و برقراری امنیت در اقصی نقاط جغرافیایی هر کشوری در عمل امکان‌پذیر نیست. بسیاری از کشورها با سرمایه گذاری به موقع و مناسب در تلاش بر افزایش امنیت سایبری و فیزیکی در حوزه‌های گوناگون اجتماعی، فرهنگی، سیاسی، نظامی، انرژی، اقتصادی، بانکی، مالی، تجاری، حمل و نقل، گردشگری، صنعت و سایر موارد هستند.

ایجاد امنیت و نظارت مناسب هزینه نیست یک سرمایه‌گذاری در کاهش ریسک، افزایش کارآیی و آرامش است!

شاهد هستیم که کشورهایی نظیر چین، امریکا، انگلیس، هند، کشورهای حاشیه خلیج فارس و کشورهای اروپایی در این زمینه بسیار فعال و پیشرو هستند. اگر به تعداد دوربین‌های نصب شده در شهرهای مختلف دنیا مراجعه کنیم، خواهیم دید که هیچ شهری از ایران در لیست ۲۰۰ شهر اول دنیا از لحاظ تعداد دوربین به نسبت جمعیت و تعداد دوربین در واحد سطح نیست. این مهم نیاز به توجه و محیط مناسب برای پوشش و توسعه دارد .

پلتفرم ابریکَم (Abricam)

طراحی و اجرای محیط و ساختار پایه‌ای رایانش ابری همراه با اجرای پلتفرم ابریکم بصورت اختصاصی بخشی از خدمات این شرکت است .

استفاده و بکارگیری از رایانش ابری در حوزه نظارت و پایش تصویری در حال توسعه و افزایش است و بر همین اساس طراحی، برنامه‌نویسی و پیاده‌سازی این مهم از سال ۱۳۹۸ شمسی در دستور کار این شرکت قرار گرفته و در حال حاضر پلتفرم ابریکم بعنوان یک VSaaS (Video Surveillance as a Service) حرفه‌ای و یا بعبارتی Cloud VMS بصورت ابر عمومی و اختصاصی فعال است. توجه به شرایط دیتاسنترها، انتقال داده‌ها، امنیت سایبری، دوربین‌های داخلی و خارجی و اتصال به سایر سیستم‌های عملیاتی و کاربردی و نیازهای کشور، اصول طراحی پلتفرم ابریکم را تشکیل داده‌اند. ابریکم با هدف ایجاد محیطی امن، پایدار و قابل توسعه برای پایش و نظارت تصاویر دوربین‌های مداربسته برای سازمان‌های بزرگ با تعداد سایت و دوربین‌های زیاد طراحی و تولید شده است.

ابریکم براساس استانداردهای رایانش ابری (Cloud Native Technologies) طراحی و پیاده‌سازی شده است. استفاده از روش‌های توسعه‌پذیر نظیر Edge Processing، Open Device، Open Platform، Kubernetes و Cyber Security همراه با عدم وابستگی به برند و مدل دوربین‌ها و تجهیزات سخت‌افزاری و مهمتر از همه انجام کلیه امور طراحی و تولید در داخل کشور، این پلتفرم را برای پوشش نیازهای داخلی مهیا کرده است.

ابریکم از بیش از ۳۰۰۰+ مدل دوربین مداربسته و ۷۰+ برند داخلی و خارجی پشتیبانی می‌کند

مزایای ابریکم

برخی از مزایای استفاده از پلتفرم ابریکم به شرح زیر است :

- عدم وابستگی به نوع و برند دوربین‌ها و استفاده از دوربین‌های موجود
- پوشش کامل استاندارد ONVIF و RTSP
- دارا بودن بیش از ۳۰۰۰ درایور اختصاصی دوربین‌ها از ده‌ها برند
- استفاده از VMS/NVR/DVR های موجود برای دوره گذر به ابریکم
- مدیریت منابع از جهت امنیت سایبری در کنترل و دسترسی به منابع
- عدم محدودیت در تعداد دوربین و سایت‌های تحت پوشش در کشور
- عدم محدودیت در میزان فضای ذخیره‌سازی برای نگهداری تصاویر
- ساختار تکرارپذیر با جایگزینی اتوماتیک (Disaster Recovery)
- استفاده از رمزگذاری براساس الگوریتم‌های عمومی یا اختصاصی
- مدیریت، ثبت و مانیتورینگ و کنترل لایه‌ای دسترسی و فعالیت‌های افراد
- مدیریت، ثبت و مانیتورینگ و کنترل لایه‌ای نرم‌افزارها و آلارم‌ها
- برنامه‌ریزی تنظیمات خاص برای مراسم، حوادث، موقعیت‌ها و بحران‌ها
- مانیتورینگ و کنترل میزان مصرف منابع در شبکه و تجهیزات سخت‌افزاری
- امنیت سایبری و فیزیکی بالا با کاهش تعداد نقاط خطرپذیر
- اتصال به سایر نرم‌افزارها نظیر پردازش تصاویر، دسترسی و آتش نشانی

کاهش هزینه‌های نگهداری، نیروی‌انسانی، توسعه، بروزرسانی سیستم عامل‌ها، نرم‌افزارها، تجهیزات سخت‌افزاری و آموزش از نتایج استفاده از ابریکم است.

ابریکم در نظارت و کنترل محل های خطرناک و ناسالم محیطی نیز کاربرد دارد. نظیر سایت‌های هسته‌ای، سایت‌های شیمیایی، سایت‌های با درجه حرارت بالا و نظایرهم

رمزنگار ابریکم

رمزنگار ابریکم یک وسیله سخت‌افزاری مطمئن برای دریافت و ارسال تصاویر، صدا و داده‌های دوربین‌ها بر روی خطوط و شبکه‌های ارتباطی به صورت رمزگذاری شده است. با استفاده از الگوریتم‌های پیچیده و حرفه‌ای و متناسب با ماهیت دوربین‌های مداربسته، رمزنگار ابریکم با بستن حفره‌های امنیتی و رمز نمودن تصاویر و اطلاعات، احتمال دسترسی‌های غیرمجاز به دوربین‌ها را به کمترین حد ممکن می رساند. هر دستگاه رمزنگار ابریکم امکان پوشش همزمان ۱۶-۳۲ دوربین مداربسته را فراهم می‌آورد.

رمزنگار ابریکم به برند و مدل دوربین وابسته نبوده و بیش از ۳۰۰۰+ مدل دوربین و ۷۰+ برند معتبر داخلی و خارجی را پوشش می‌دهد.

از دیگر مزایای استفاده از رمزنگار ابریکم، امکان نگهداری تصاویر دوربین‌ها در زمان قطع خطوط و شبکه ارتباطی است. این محصول با ایجاد یک فضای ذخیره‌سازی لبه (Edge Storage) نگهداری تصاویر در زمان قطع ارتباط و ارسال اتوماتیک آنها بعد از اتصال را به ابریکم فرآهم آورده است.

زمان حملات سایبری را ما تعیین نمی‌کنیم ولی میزان هوشیاری و آمادگی در اختیار ما است!

استفاده از ابریکم

ابریکم برای استفاده توسط کاربران و گروه‌های زیر طراحی شده است:

ابریکم عمومی: این پلتفرم قادر است تا نیازهای کاربران خانگی، شرکت ها و مراکز کوچک را پشتیبانی نماید. پیچیدگی استفاده و نگهداری از تجهیزات و امکان خرابی و سرقت دستگاه‌های ضبط در مقایسه با امکانات و دسترسی آسان از مهمترین عوامل در روی آوردن کاربران به استفاده از ابریکم عمومی است.

به وب سایت ابریکم (www.abricam.ir) برای استفاده از امکانات پلتفرم در محیط وب، اندروید و iOS مراجعه کنید.

ابریکم تجاری: این بخش از بازار شامل شرکت‌ها و موسساتی متوسط به بالا است که یک یا چند سایت/مرکز عملیاتی دارند.. این دسته از کاربران نیز با مراجعه به سایت ابریکم (www.abricam.ir) و تکمیل فرم درخواست می‌توانند از امکانات و خدمات این پلتفرم در زمانی کوتاه بهره‌برداری نمایند. استفاده براساس روش‌های Hosting و بصورت امن انجام می شود. کاهش هزینه‌ها، تنوع خدمات، استفاده از محیط با لوگو شرکت و امنیت سایبری مناسب از عوامل اصلی در استفاده از ابریکم تجاری است.

استفاده مناسب از دوربین های مداربسته در منازل و فروشگاه‌ها می تواند تا ۶۷٪ میزان سرقت‌ها را کاهش دهد.

ابریکم اختصاصی: سازمان‌های بزرگ با هزاران دوربین و سایت‌های متعدد که دیتاسنتر هم دارند با ایجاد و راه اندازی ابریکم اختصاصی در دیتاسنترهای خود قادر خواهند بود تا علاوه بر ایجاد امنیت بهتر در کاهش هزینه‌ها نیز قدم بزرگی را بردارند. اجرای چنین پروژه‌هایی براساس استفاده بهینه از شرایط و امکانات موجود و طراحی یک روند مهاجرت از شرایط فعلی به شرایط رایانش ابری انجام می‌شوند.

اجرای ابریکم اختصاصی

ابریکم براساس استفاده از آخرین دستاوردهای فشرده‌سازی، انتقال، ضبط و مدیریت منابع ویدیویی در زمینه پایش تصاویر و با بکارگیری مناسب‌ترین میزان پهنای باند برای انتقال تصاویر طراحی شده است.
برخی از موارد مهمی که برای پیاده سازی ابریکم در سازمان‌های بزرگ مد نظر قرار گرفته عبارتند از:

۱- سازمان‌های بزرگ در یک دوره زمانی طولانی اقدام به خرید تجهیزات و دوربین‌های متنوع نموده‌اند که براساس شرایط مالی و تکنولوژی‌های در دسترس، تنوع زیادی در برند و مدل دوربین ها و تجهیزات ذخیره‌سازی وجود دارد.

۲- شرایط جزیره‌ای در خصوص مدیریت و پایش تصاویر در سایت‌های آنها وجود دارد. عدم سازگاری تجهیزات با یکدیگر و محدودیت‌های ارتباطی و شرایط مدیریتی و بودجه‌ای سبب شده تا امکان داشتن یک ساختار یکپارچه کمتر میسر باشد.

۳- امکان اعمال تغییرات یکپارچه و همزمان در کلیه مراکز و سایت‌ها وجود ندارد. محدودیت‌های ارتباطی، آموزش پرسنل، خطرات ایجاد وقفه در کارها، تامین بودجه و بسیاری شرایط ریز و درشت دیگر وجود دارند که امکان مهاجرت یکباره از ساختار فعلی به ساختار ابری را ناممکن می سازد.

تغییر و بروزرسانی در حوزه فناوری اطلاعات بدلایل متعددی همواره پیچیده بوده و مهاجرت به پلتفرم های ابری از این قاعده مستثنی نیست.

طراحی ابریکم اختصاصی براساس توجه به شرایط واقعی سازمان‌ها و امکان برنامه‌ریزی و اجرای مرحله‌ای انجام شده است.

دستاوردهای بکارگیری ابریکم

ابریکم براساس استفاده از آخرین دستاوردهای فشرده‌سازی، انتقال، ضبط و مدیریت منابع ویدیویی در زمینه پایش تصاویر و با بکارگیری کمترین میزان پهنای باند برای انتقال تصاویر، امکان مدیریت، پایش و نگهداری تصاویر در دیتا سنترهای سازمانی را بصورت اختصاصی، هیبریدی و عمومی فرآهم آورده است. ابریکم اختصاصی برای سازمان‌هایی با تعداد سایت و دوربین زیاد توصیه می‌شود. در مجموعه‌هایی که نظارت تصویر آنان از طریق شبکه اختصاصی و توزیع شده صورت می گیرد، نتایج مثبت و فراوانی را شاهد خواهند بود. برخی نتایج و شرایط حاصل از بکارگیری ابریکم اختصاصی در زیر ارائه شده است.

آیا استفاده از رایانش ابری یک انتخاب است یانیاز؟

ابریکم با استفاده از روش های هوشمند در پوشش کمی و کیفی امنیت نقش بسزایی دارد.

- اجرای مرحله‌ای تا حصول ساختار ابری جامع
- عدم محدودیت در تعداد دوربین و سایت مورد نیاز
- کاهش هزینه خرید و نگهداری تجهیزات سخت‌افزاری
- مدیریت ایده‌آل کاربران، سایت‌ها و آلارم‌ها
- مدیریت نقش و عملکرد کاربران در عملیات و نظارت
- مدیریت و کنترل شبکه ارتباطی و پهنای باند
- ایجاد مانیتورینگ‌های مرکزی و محلی قابل توسعه
- عدم وابستگی به مدل و نوع دوربین open device
- استفاده از آنالیتیک دوربین‌ها edge processing
- استفاده از حافظه دوربین‌ها edge memory
- کلیه عملیات متداول در VMS و NVR های پیشرفته
- استفاده از ابریکم بریج برای افزایش امنیت سایبری
- اتصال به نرم‌افزارهای مشتریان، پرسنلی و اداری
- اتصال به نرم‌افزارهای کنترل دسترسی و IoT
- اتصال به نرم‌افزارهای آتش نشانی و حسگرهای فیزیکی
- ساختار open platform برای ایجاد سیستم جامع
- پرتال‌های مخصوص مدیران، ادمین و کاربران
- کلاینت بصورت وب، iOS & Android App
- کاهش چشمگیر هزینه‌های بروزرسانی و نگهداری
- گسترش سریع حوزه‌های جغرافیایی تحت پوشش
- تجمیع تصاویر انتخابی براساس حوزه جغرافیایی
- پردازش و آنالیز تصویر و سیستم‌های هوش مصنوعی

چه سازمان‌هایی می‌توانند از ابریکم اختصاصی استفاده کنند؟

هر مجموعه و سازمانی با توجه به ماهیت و ساختار خود دارای نیازمندی‌های متفاوت و متنوعی است. افتخار داریم که اعلام کنیم که با دانش فنی، تجربه و تنوع محصولات، نیازها و کاربری‌های متنوع را در بخش‌های گوناگون برآورده ساخته‌ایم. در این راستا با امکان اعمال تغییرات، شرایط منحصربفرد هر سازمان را مورد توجه قرار داده و پلتفرم را برآن اساس تنظیم و تحویل می دهیم. برای کسب اطلاعات بیشتر با واحد فروش شرکت ۰۲۱-۸۸۷۰۲۰۷۰ تماس حاصل فرمایید.

طراحی، پیاده سازی، تامین تجهیزات، آموزش و راه‌اندازی محیط رایانش ابری و پلتفرم ابریکم بصورت کلید در دست (Turn Key) توسط شرکت پردازش تصویر قابل انجام است.

- بانک‌ها و موسسات مالی و اعتباری
- دانشگاه‌ها و مراکز آموزشی
- شهرک‌ها، مراکز صنعتی و تولیدی
- مراکز نظامی، انتظامی و مرزی
- مراکز تجاری و اداری
- مراکز حساس و امنیتی
- اصناف و اتاق‌های بازرگانی
- مراکز و سایت‌های مخابراتی
- شرکت‌های بیمه و بورس
- فرودگاه‌ها و ترمینال‌های مسافری
- بنادر و پایانه‌های حمل و نقل
- موزه‌ها، مراکز تفریحی و گردشگری
- مراکز قضایی و تادیبی
- دفاتر داخل و خارج از کشور
- شهرداری‌ها و سازمان‌های عمومی
- استادیوم‌ها و مراکز ورزشی
- استانداری‌ها و فرمانداری‌ها
- پتروشیمی‌ها، سایت‌های نفت و گاز
- ترافیک، امنیت شهری و جاده‌ها
- بیمارستان‌ها و مراکز بهداشتی
- شهر هوشمند

شرکت پردازش تصویر کمان

www.kaman.ir

پلتفرم ابریکم

www.abricam.ir

۰۲۱ ۸۸۷۰ ۲۰۷۰

www.kaman.ir

info@kaman.ir

تهران، خیابان مطهری، خیابان میرزای شیرازی،
خیابان نعیمی، پلاک ۱۹،ساختمان کمان