گزارش امنیت سامانه‌های ابری

VER: 1.04

2019

CLOUD SECURITY REPORT

پارس آوان
امنیت شبکه و اطلاعات

پیش‌گفتار

امروزه شرکت‌ها به منظور بهره‌گیری از مزایای رایانش ابری همچون افزایش بهره‌وری، مقیاس‌پذیری و چابکی، به سرعت در حال پذیرش و انتخاب این فناوری هستند.
هر چند ارایه دهندگان سرویس‌های ابری همچون وب سرویس‌های آمازون (AWS)، مایکروسافت آژور و پلتفرم گوگل کلود (GCP) در حال گسترش سرویس‌های امنیتی جهت محافظت از پلتفرم‌های ابری رو به رشد خودشان هستند، اما این مسئولیت مشتریان است که برنامه‌های کاربردی و داده‌های خودشان را در این محیط‌های ابری امن‌سازی کنند.

در گزارش امنیت ابر ۲۰۱۹ مشخص شده که چه روش‌هایی برای امن‌سازی داده‌ها، سیستم‌ها و سرویس‌های ابر در مدل مسئولیت مشترک خوب کار می‌کنند و چه روش‌هایی خیر. نتایج این مطالعه، ادامه‌ای بر چالش‌های گذشته است:

- مهم‌ترین دغدغه برای کارشناسان امنیت سایبری مربوط به مخاطره نشت ابر و از دست رفتن داده‌ها است (۶۴ درصد).
- بزرگترین موانع برای پذیرش راهکارهای ابری عبارتند از امنیت داده‌ها، خطر نشت و از دست رفتن داده‌ها (۲۹ درصد) و خطرات امنیتی کلی (۲۸ درصد).
- ۴۳ درصد اعلام کرده‌اند که چالش برانگیزترین بخش فرایند تطبیق یافتن با استانداردهای قانونی، نظارت بر آسیب پذیری‌های جدید در سرویس‌های ابری است.

در مجموع، یافته‌های این گزارش حاکی از این است که تیم‌های امنیتی برای حفاظت از محیط رو به رشد فناوری اطلاعات و تکامل خودشان باید راهبردها و وضعیت امنیتی را ارزیابی دوباره کرده و با نقص‌های روش‌ها و ابزارهای امنیتی قدیمی مقابله کنند.

روش‌شناسی و داده‌های آماری

روش‌شناسی و داده‌های آماری

گزارش امنیت ابر سال ۲۰۱۹ مبتنی بر نتایج یک نظرسنجی آنلاین جامع از کارشناسان حوزه امنیت سایبری است که در ماه مارس سال ۲۰۱۹ جهت به دست آوردن درکی عمیق نسبت به جدیدترین گرایش‌ها، چالش‌های کلیدی و راهکارها در حوزه امنیت فناوری ابری انجام شده است. طیف پاسخ دهندگان از مدیران اجرایی فنی تا مسئولین امنیت فناوری اطلاعات متغیر بوده و در آن از افراد سازمان‌هایی با ابعاد مختلف در چندین صنعت نظرسنجی شده است.

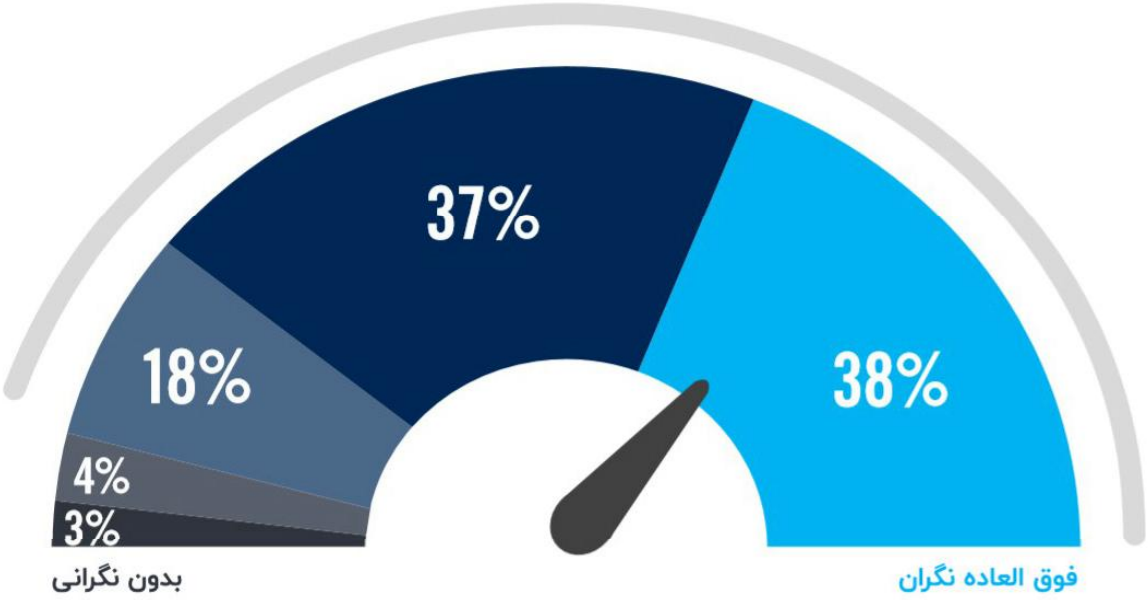
امنیت در ابرهای عمومی

امنیت در ابرهای عمومی

در حالی که میزان پذیرش و استفاده از ابرهای عمومی رو به افزایش است، هیچ نشانه‌ای از کاهش نگرانی‌های امنیتی مشاهده نمی‌شود. بیشتر کارشناسان امنیت سایبری (۹۳ درصد) می‌گویند نگرانی آنها درباره امنیت ابر عمومی حداقل در سطح متوسط قرار دارد، که این عدد نسبت به سال گذشته کمی افزایش پیدا کرده است.

در رابطه با امنیت ابرهای عمومی چقدر نگرانی دارید؟

93% درصد سازمان‌ها نسبت به امنیت ابر، نگرانی متوسط تا شدیدی دارند.



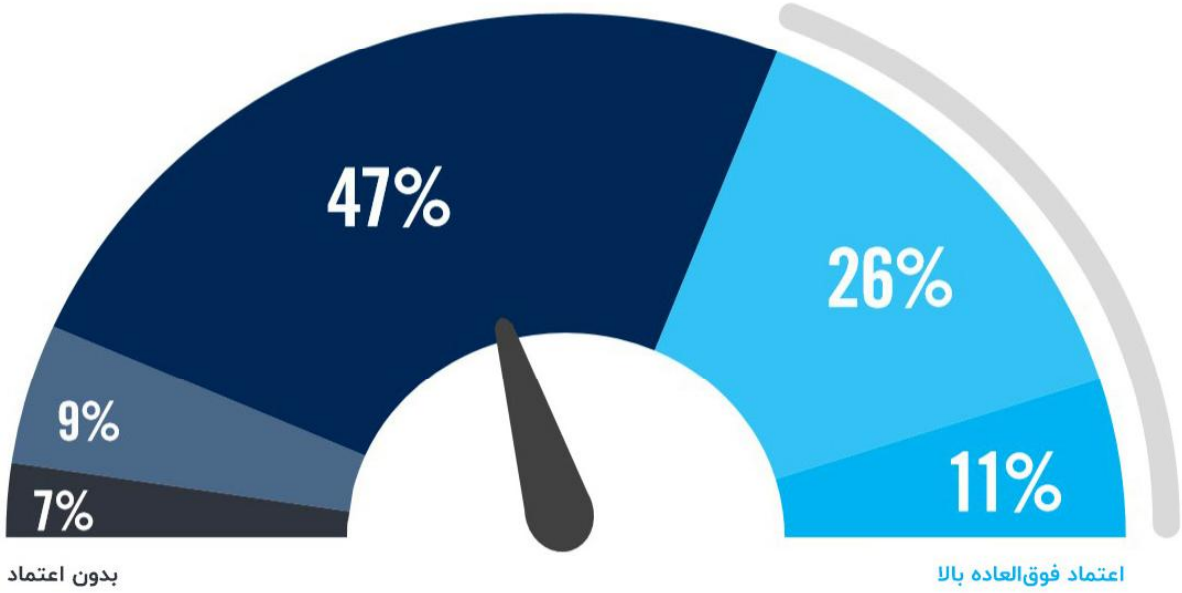
ضریب اطمینان فناوری ابری

ضریب اطمینان فناوری ابری

بیشتر سازمان‌ها نسبت به وضعیت امنیت ابری خودشان حداقل اطمینانی متوسط دارند (۸۴ درصد). شاید این امر نشان دهنده وجود اعتماد بیش از حد باشد که چالش‌ها و حوادث امنیتی بیان شده در این گزارش چنین موضوعی را تأیید می‌کند.

نسبت به امنیت سازمان خودتان در خصوص وضعیت امنیت ابر چقدر اطمینان دارید؟

37% تنها یک سوم، نسبت به وضعیت امنیت ابر سازمان خودشان اطمینان زیاد یا فوق‌العاده زیادی دارند

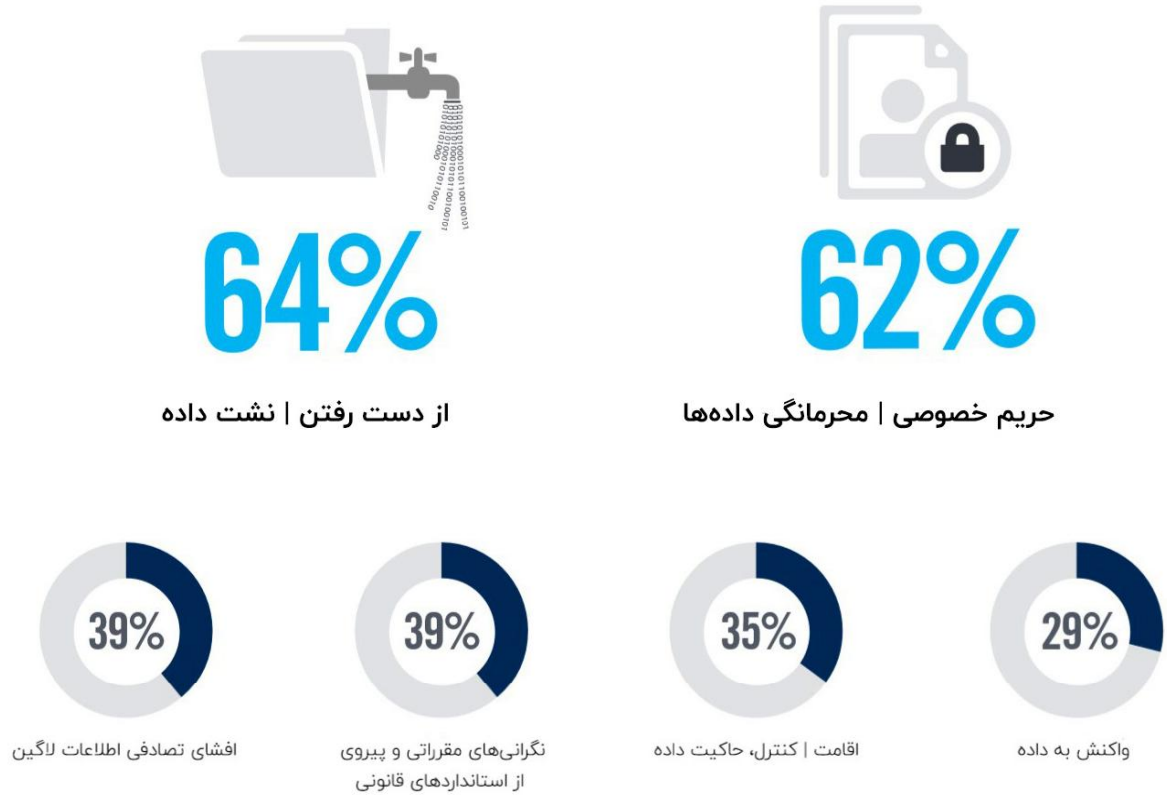


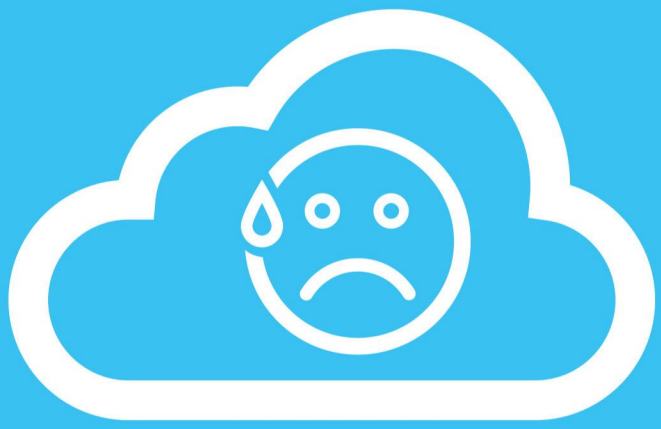
نگرانی‌های امنیت فناوری ابری

نگرانی‌های امنیت فناوری ابری

هر چند ارایه دهندگان سرویس‌های ابر، راهکارهای امنیتی ارایه می‌دهند که روز به روز قوی‌تر نیز می‌شوند اما در نهایت، مشتریان خودشان مسئول امن‌سازی فعالیت‌هایشان در فضای ابری هستند. اصلی‌ترین چالش‌های امنیت ابر در این نظرسنجی مربوط به از دست دادن داده‌ها (۶۴ درصد) و حریم خصوصی داده‌ها (۶۲ درصد) بود. پس از آن نگرانی‌های مربوط به انطباق با قوانین (۳۹ درصد) و افشای تصادفی اطلاعات لاگین (۳۹ درصد) قرار دارد.

بزرگترین نگرانی‌های شما درباره امنیت ابر چیست؟





دردسرهای امنیت اطلاعات

دردسرهای امنیت اطلاعات

با حرکت هر چه بیشتر بار کاری به سمت ابر، کارشناسان امنیت سایبری متوجه پیچیدگی محافظت از این بار کاری می‌شوند. دو دردسر امنیتی اصلی که مراکز عملیاتی امنیت با آن روبرو هستند پیروی از استانداردها (۳۴ درصد) و عدم وجود دید کافی نسبت به امنیت زیرساخت‌ها (۳۳ درصد) است. تنظیم خط‌مشی‌های امنیتی یکپارچه در سراسر محیط ابر و محیط‌های داخلی (۳۱ درصد) و نداشتن کارمندان باصلاحیت در حوزه امنیت (۳۱ درصد) جایگاه بعدی را به خود اختصاص می‌دهند.

بزرگترین دردسرهای عملیاتی روزمره ناشی از تلاش برای محافظت از ابر چیست؟

33%

دید لازم نسبت به امنیت زیرساخت

34%

پیروی از استانداردها

واکنش به داده

حوزه امنیت نمی‌تواند خودش را با سرعت تغییراتی که به برنامه‌های کاربردی جدید یا موجود اعمال می‌شود، همگام کند.

نداشتن کارمندان باصلاحیت

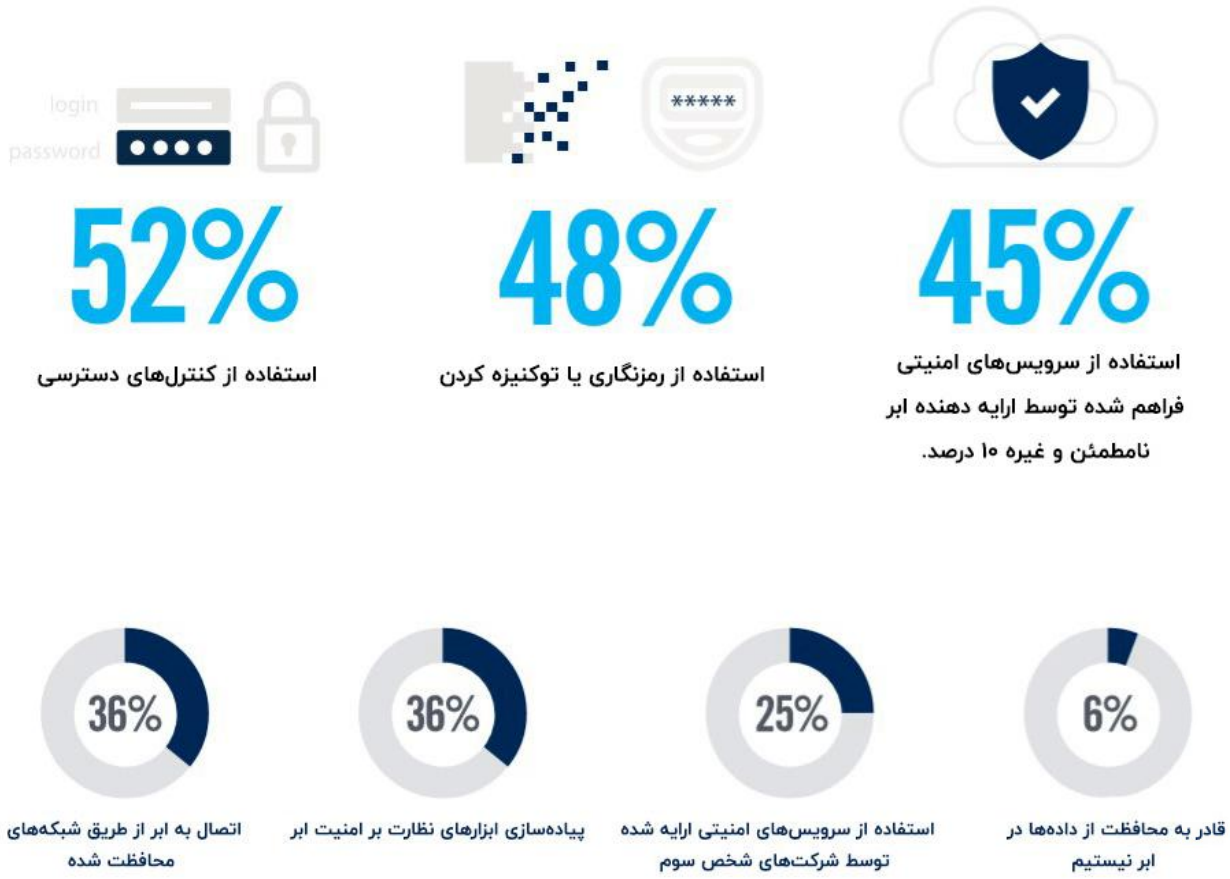
تنظیم خط‌مشی‌های امنیتی یکپارچه

محافظت از داده‌ها در فناوری ابری

محافظت از داده‌ها در فناوری ابری

با افزایش میزان استفاده از ابر، حجم داده‌های ذخیره شده در محیط‌های ابری نیز افزایش یافته است. برای سومین سال پیاپی کارشناسان امنیت سایبری اعلام کرده‌اند که کنترل‌های دسترسی (۵۲ درصد) روش اصلی است که از آن جهت محافظت از داده‌ها در ابر استفاده می‌کنند و بعد از آن رمزنگاری یا توکنیزه کردن (۴۸ درصد)، استفاده از سرویس‌های امنیتی فراهم شده توسط ارایه دهنده ابر (۴۵ درصد)، پیاده‌سازی ابزارهای نظارت بر امنیت ابر (۳۶ درصد) و اتصال به ابر از طریق شبکه‌های محافظت شده (۳۶ درصد) قرار دارند.

چگونه از داده‌ها در ابر محافظت می‌کنید؟



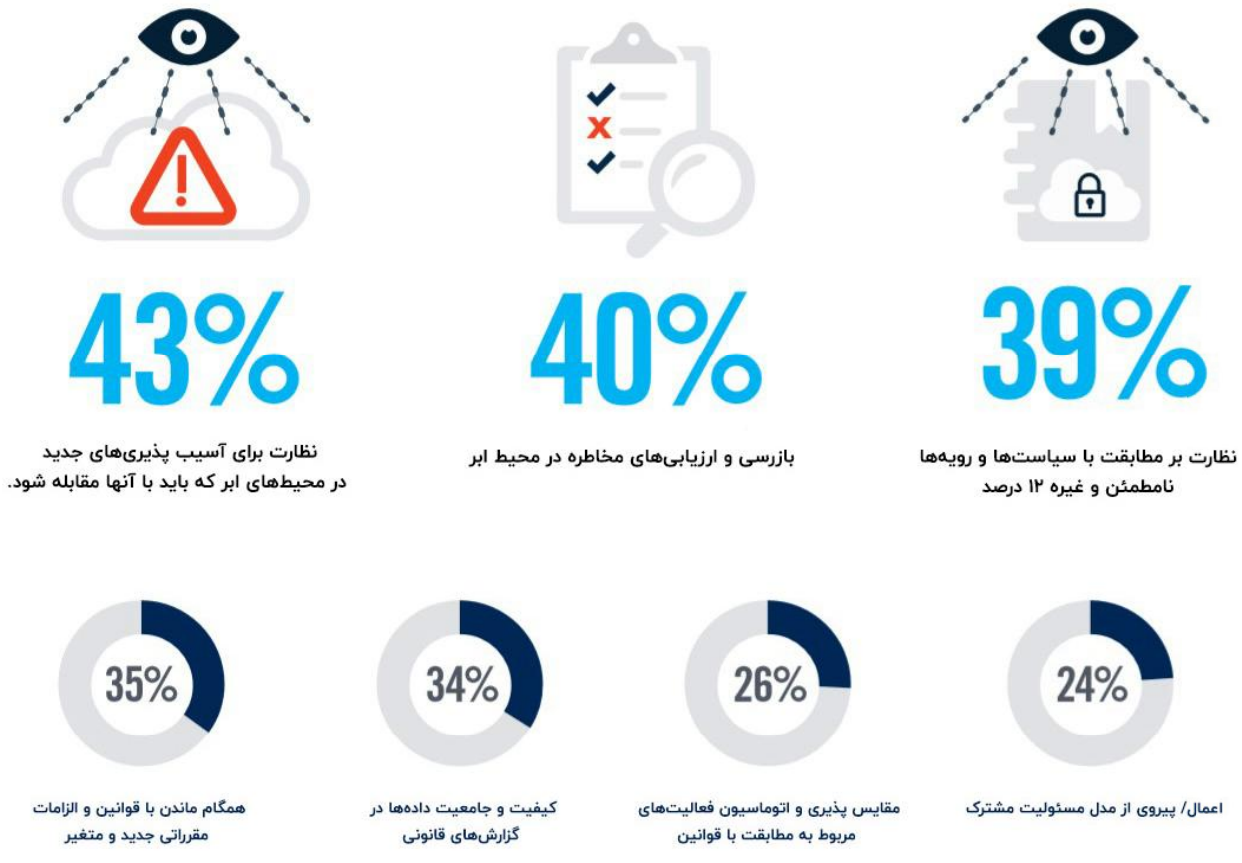
ISO

چالش‌های انطباق با استانداردهای قانونی

چالش‌های انطباق با استانداردهای قانونی

در خصوص چالش‌های مطابقت با استانداردهای قانونی، نظارت بر سرویس‌های ابری برای مقابله با آسیب پذیری‌های جدید با ۴۳ درصد در جایگاه اول قرار دارد و بعد از آن ارزیابی مخاطره و بازرسی (۴۰ درصد) و نظارت بر پیروی از استانداردهای قانونی قرار دارد (۳۹ درصد).

کدام بخش از مطابقت با استانداردهای قانونی ابر چالش برانگیزتر است؟



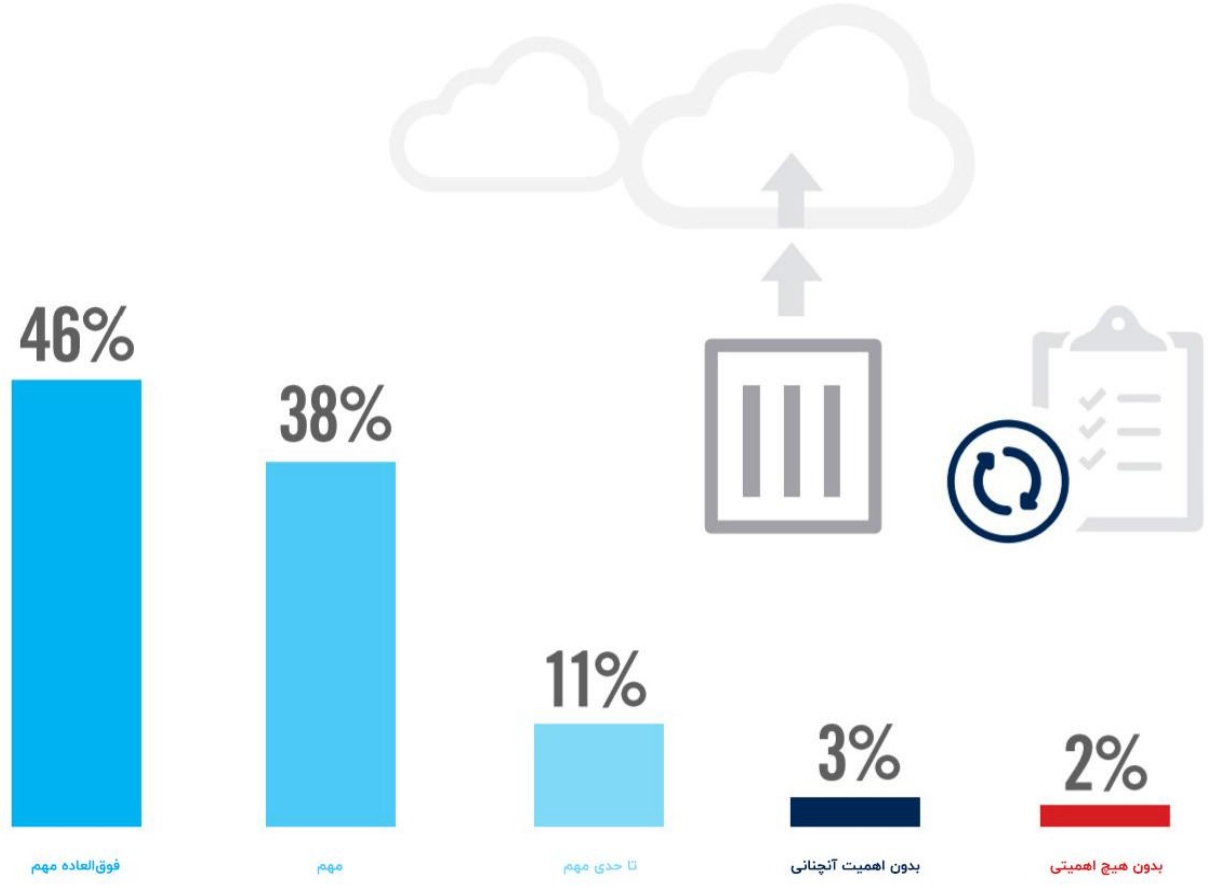
ISO

انطباق مستمر با استانداردهای قانونی

انطباق مستمر با استانداردهای قانونی

بیشتر سازمان‌هایی (۹۵ درصد) که کارهای داخلی را امن‌سازی می‌کنند، حفظ مطابقت با استانداردهای قانونی در هنگام مهاجرت بار کاری به ابر را فوق‌العاده مهم (۴۶ درصد)، بسیار مهم (۳۸ درصد) یا تا حدی مهم (۱۱ درصد) تلقی می‌کنند.

اگر بار کاری خودتان (ماشین‌های مجازی) را به صورت داخلی امن‌سازی می‌کنید، حفظ انطباق مستمر با استانداردهای قانونی در هنگام مهاجرت آنها به ابر چقدر اهمیت دارد؟

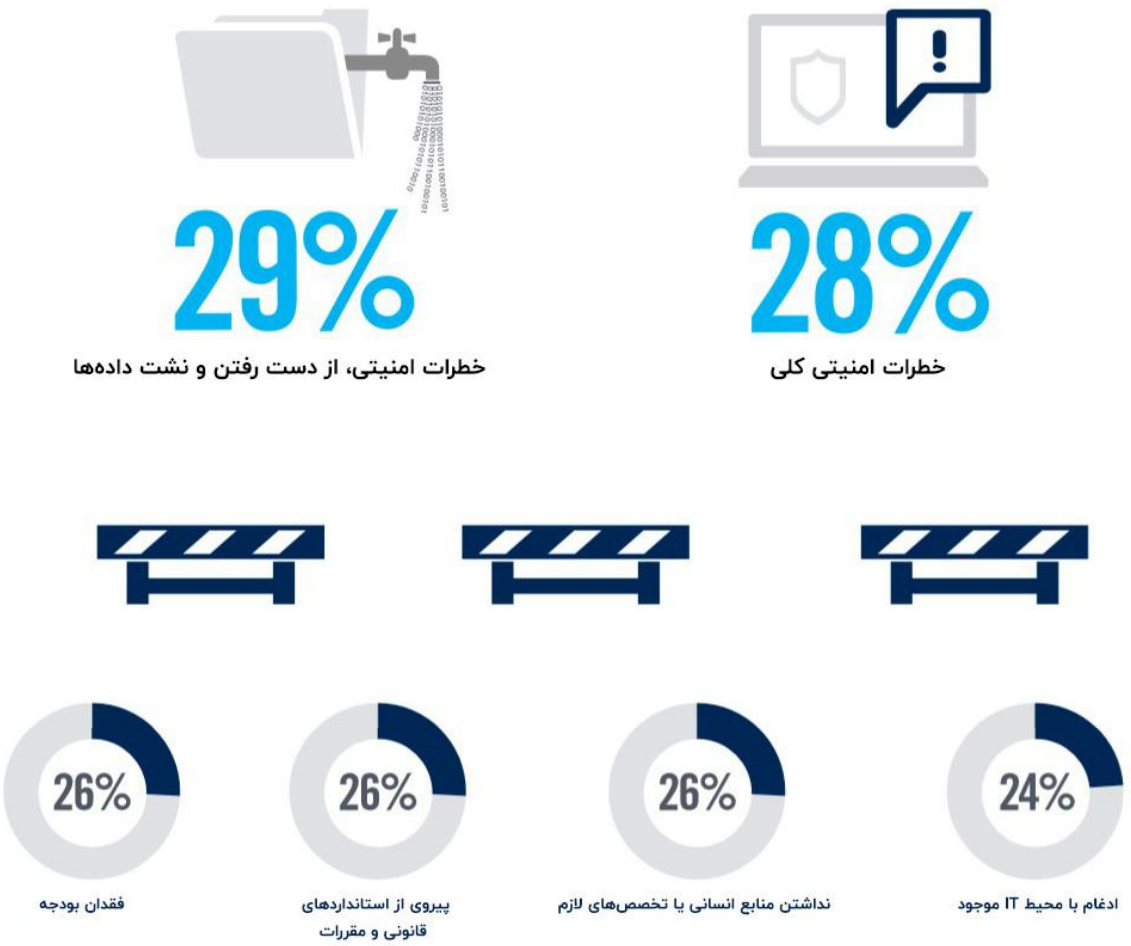


موانع پذیرش فناوری ابری

موانع پذیرش فناوری ابری

رایانش ابری با وجود تمام مزایا باز هم بدون چالش نیست. امنیت داده‌ها (۲۹ درصد) و خطرات امنیتی کلی (۲۸ درصد)، همراه با نداشتن بودجه (۲۶ درصد)، چالش‌های مربوط به مطابقت با استانداردهای قانونی (۲۶ درصد) و نداشتن کادر باصلاحیت (۲۶ درصد) در بالای لیست موانع پذیرش سریع ابر قرار دارند.

بزرگترین موانع برای پذیرش ابر در سازمان شما چیست؟



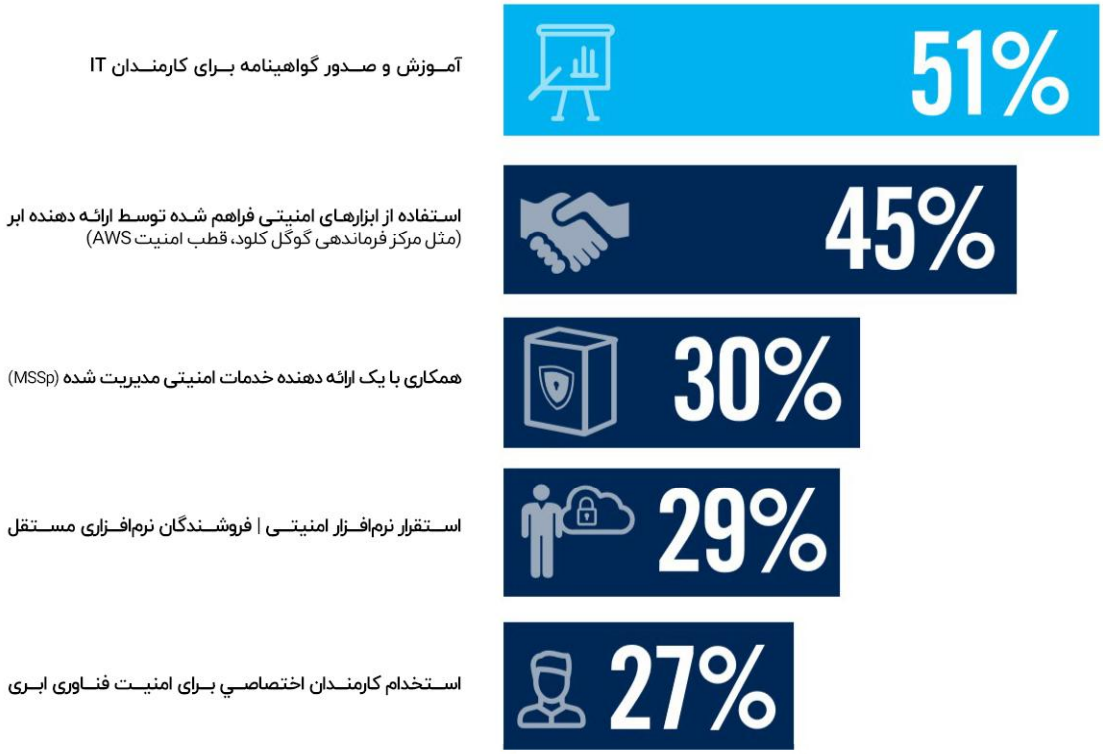
از دست دادن کنترل ۲۲ درصد | پیچیدگی مدیریت استقرار ابر ۲۰ درصد | ترس از وابستگی به فروشنده ۲۰ درصد | هزینه/ عدم وجود بازگشت سرمایه ۱۹ درصد | مقاومت‌های داخلی ۱۹ درصد | کارایی برنامه‌های کاربردی در ابر ۱۶ درصد | نداشتن شفافیت و قابلیت دید ۱۶ درصد | نداشتن قابلیت سفارشی‌سازی ۱۶ درصد | مسایل مربوط به ردیابی و صدور صورتحساب ۱۵ درصد | عدم پذیرش و حمایت از سوی مدیریت ۱۳ درصد | دسترس پذیری ۱۳ درصد | نداشتن بلوغ مدل‌های سرویس ابر ۱۳ درصد | نداشتن رضایت نسبت به پیشنهادهای سرویس ابر/ کارایی/ قیمت‌ها ۱۱ درصد | پشتیبانی نکردن از سوی ارایه دهنده ابر ۱۰ درصد | غیره ۴ درصد.

راه‌های افزایش امنیت ابر

راه‌های افزایش امنیت ابر

برای سومین سال پیاپی، آموزش و صدور گواهینامه برای کارمندان فناوری اطلاعات (۵۱ درصد) مهم‌ترین تاکتیکی است که سازمان‌ها برای اطمینان از برآورده شدن نیازهای امنیتی رو به رشد خودشان پیاده‌سازی می‌کنند. ۴۵ درصد از پاسخ دهندگان به ابزارهای امنیتی فراهم شده توسط ارایه دهنده ابر متکی هستند و ۳۰ درصد با یک ارایه دهنده سرویس‌های امنیتی مدیریت شده همکاری می‌کنند تا خلاءهای احتمالی موجود در قابلیت‌ها و توانایی‌ها را رفع کنند.

هنگام حرکت به سمت ابر، چگونه نیازهای امنیتی جدید خودتان را برآورده می‌کنید؟



اولویت‌های امنیت فناوری ابری

اولویت‌های امنیت فناوری ابری

در سال جاری، اولویت‌های اصلی سازمان‌ها عبارت بودند از محافظت در برابر بدافزارها (۲۵ درصد)، دستیابی به مطابقت با استانداردهای قانونی (۲۰ درصد) و امن‌سازی برنامه‌های کاربردی اصلی ابر (۱۵ درصد).

اولویت‌های امنیت ابر برای سازمان شما در سال جاری چه بوده است؟

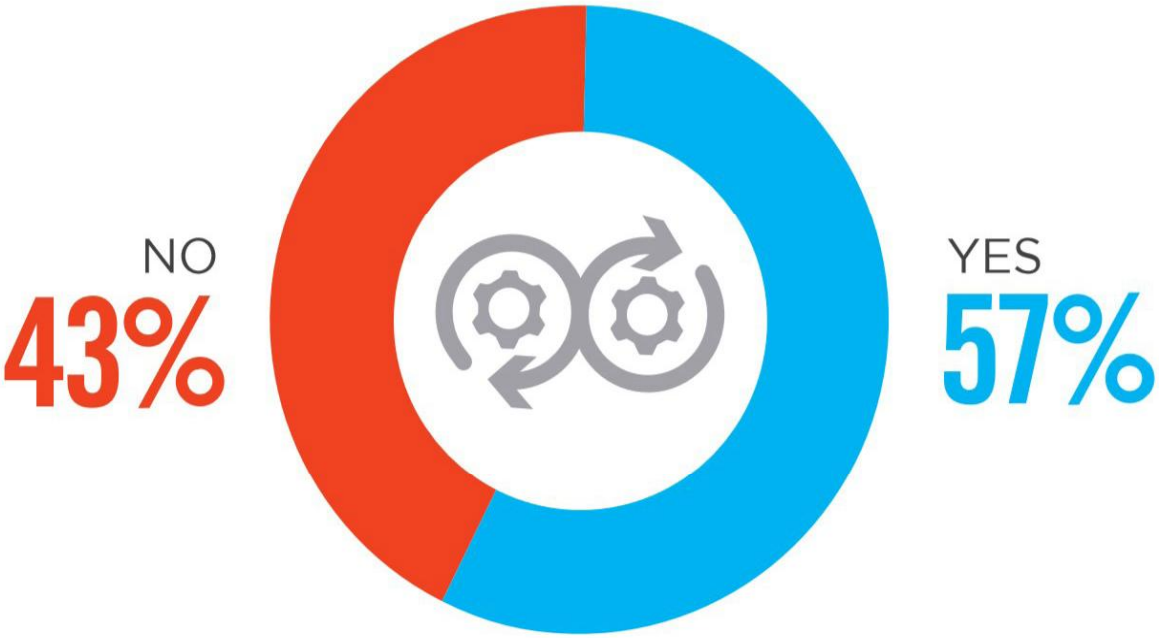
امن‌سازی خط‌مشی BYOD (دستگاه خودتان را سر کار بیاورید)، ۴ درصد.

ادغام زنجیره ابزار DevOps

ادغام زنجیره ابزار DevOps

بیشتر سازمان‌ها برای توسعه و تحویل سریع‌تر نرم افزارها همزمان با بهبود امنیت و کیفیت برنامه‌های کاربردی از DevOps استفاده می‌کنند. یک زنجیره ابزار DevOps متشکل از مجموعه‌ای از ابزارهای توسعه است که برای پشتیبانی از کارهای توسعه، عملیات و تحویل استفاده می‌شود.
وقتی از کارشناسان فناوری اطلاعات سؤال شد که آیا زنجیره ابزار DevOps را در پیاده‌سازی‌های ابرشان ادغام می‌کنند، از بین تمام پاسخ دهندگان ۵۷ درصد گفتند بله و ۴۳ درصد گفته‌اند خیر.

هنگام حرکت به سمت ابر، چگونه نیازهای امنیتی جدید خودتان را برآورده می‌کنید؟

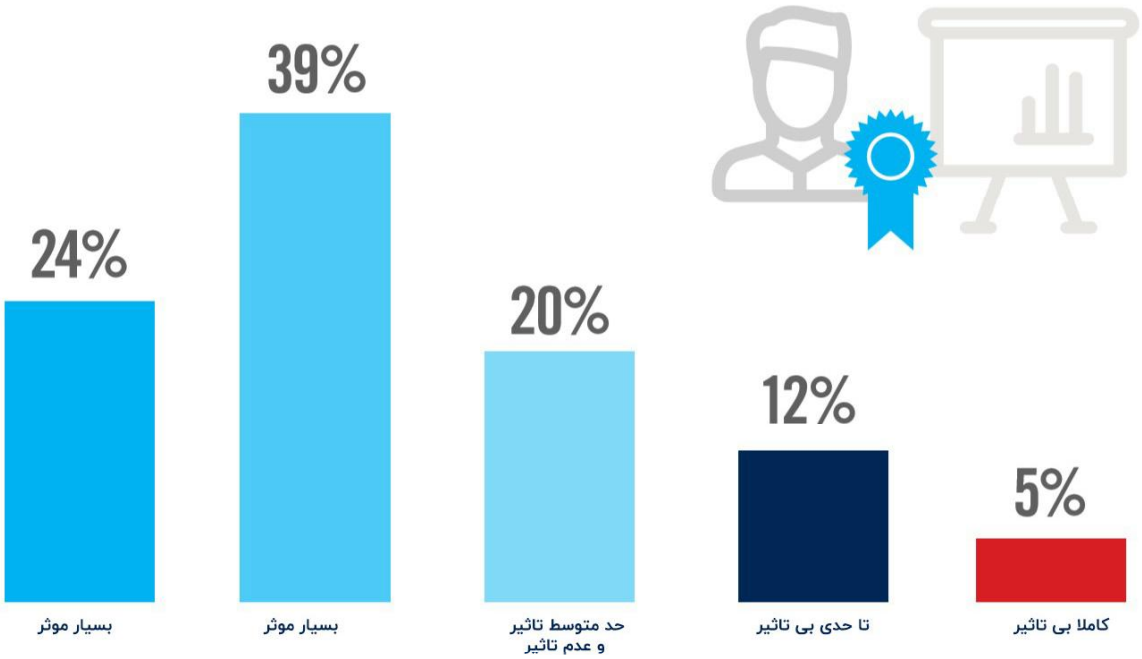


برنامه آموزش امنیت فناوری ابری

برنامه آموزش امنیت فناوری ابری

از نظر بیشتر سازمان‌ها (۶۳ درصد) برنامه‌های آموزش امنیت فعلی آنها بسیار کارآمد (۲۴ درصد) یا تا حدی کارآمد (۳۹) هستند.

برنامه آموزش امنیت فعلی شما چقدر کارآمد است؟

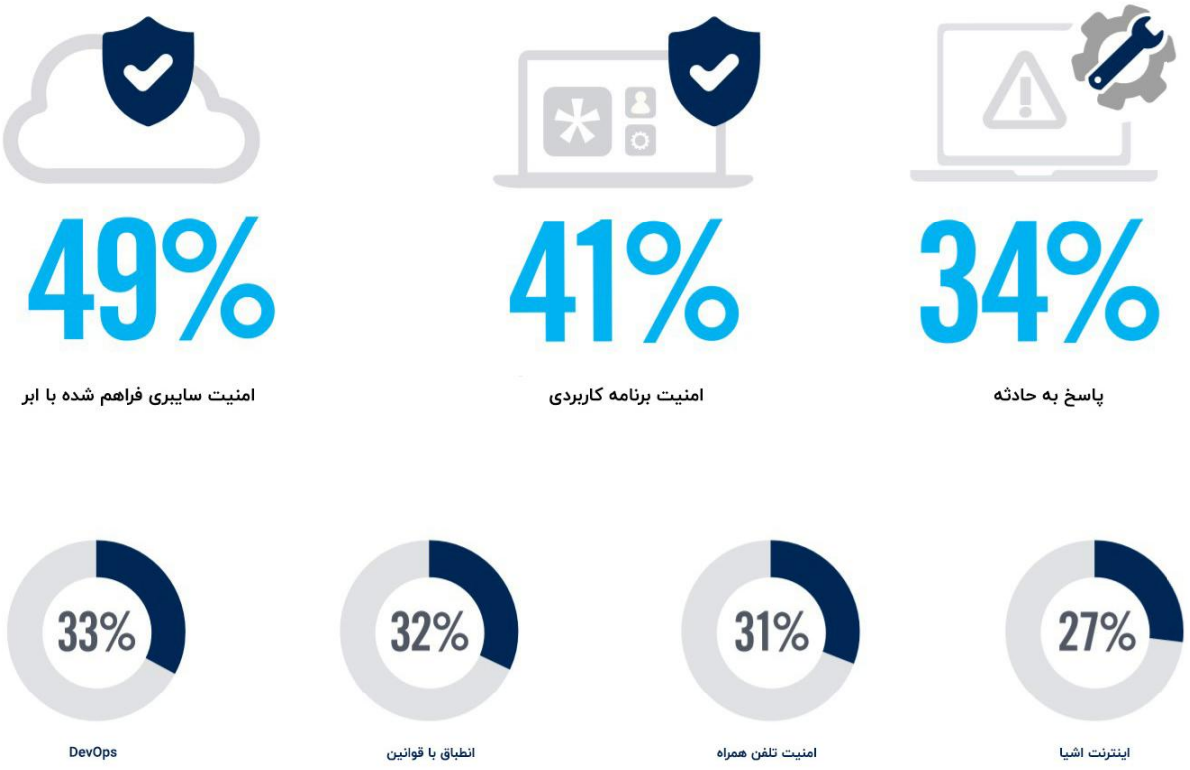


تمرکز آموزش امنیت

تمرکز آموزش امنیت

در رابطه با اولویت دادن به موضوع‌های مربوط به آموزش امنیت، شرکت کنندگان این نظرسنجی اول امنیت سایبری فراهم شده با ابر (۴۹ درصد) و سپس امنیت برنامه‌های کاربردی (۴۱ درصد) و پاسخ به حوادث (۳۴ درصد) را انتخاب کردند.

کدام یک از موضوعات زیر را برای موفقیت در آموزش و آموزش مداوم برای موفقیت در نقش فعلی خود مهم‌تر می‌دانید؟



مهارت‌های نرم (رهبری، کار تیمی مؤثر، برقراری ارتباط برای متقاعد کردن و آموزش) ۲۶ درصد / چارچوب‌های مبتنی بر مخاطره ۲۵ درصد / آسیب پذیری‌های کد باز ۲۵ درصد / جرم‌شناسی‌های قانونی ۲۴ درصد / تشخیص فیشینگ/ مهندسی اجتماعی ۲۲ درصد | PII ۱۸ درصد / نامطمئن/ غیره ۴ درصد.

CLOUD SECURITY REPORT 2019

www.ParsAvan.com | (۰۲۱) ۹۱۰۰۵۴۱۸ | Sales@ParsAvan.com