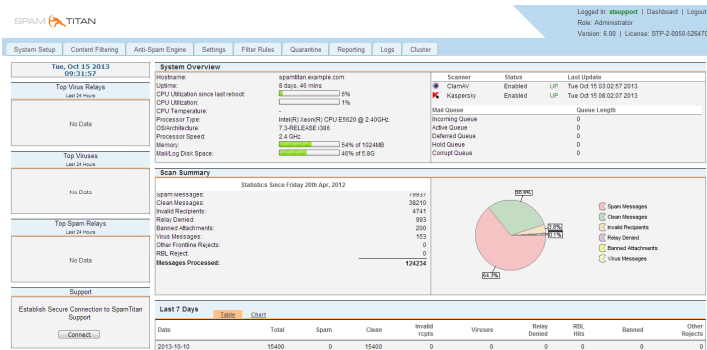




- آنالیز چند لایه ضد اسپم که منجر به افزایش دقت تشخیص به بالاتر از ۹۸٪ می شود.
- نرخ تشخیص اشتباه کمتر از ۳٪
- مجهز به دو موتور ضد ویروس
- مدیریت تحت وب و گزارشگیری زنده
- نصب، مدیریت و نگهداری آسان
- قابل ارائه به صورت دستگاه فیزیکی و یا به صورت مجازی و یا ابری



### معرفی

### چرا از اسپم تایتان استفاده می کنیم؟

اسپم تایتان بصورت هدفمند ساخته شده است تا بتواند به مشاغل کمک کند تا با راحتی از کاربران و شبکه خود در برابر ایمیل های ناخواسته، ویروس ها و بدافزارها محافظت کنند.

اسپم تایتان به دو صورت ابری و نصب در محل (on-premise) به شکل دروازه ایمیل، ارائه می شود.

راه حل ابری گونه ای طراحی شده تا با راحتی در زیرساخت های موجود ادغام شود و گسترش آن بسیار ساده است. اسپم تایتان ابری به کسب و کارها این امکان را می دهد که ترافیک ایمیل سازمان را بدون هزینه های اضافی یا صرف وقت، فیلتر کنند.

راه حل درگاه (Gateway) در مرکز داده سازمان نصب شده و سطح دقیق تری از کنترل را برای یک مدیر سیستم امکان پذیر می کند

ایمیل یکی از ابزارهای ارتباطی حیاتی شرکتهای امروزی است که مزایای زیادی مانند افزایش بهره وری، کارایی و صرفه جویی در هزینه ها را به ارمغان می آورد. متأسفانه در کنار مزایای بسیار، ارتباطات ایمیلی با تهدیدهای مهمی گره خورده است که علاوه بر توانایی تخریب شبکه شما، ممکن است پیامدهای جدی حقوقی و مالی برای شما و تجارت شما به همراه داشته باشد. اقدام ساده باز کردن ایمیل و یا کلیک بر روی یک لینک می تواند ویروس ها را آزاد کند که علاوه بر تخریب ساختارهای داخلی شبکه شما، می تواند پیامدهای ویرانگری را برای کلاینت ها به همراه داشته باشد.

SpamTitan (اسپم تایتان)، با مدیریت ترافیک ایمیل سازمان و با مسدود کردن نامه های ناخواسته، ویروس ها و بدافزارها، سازمان را در برابر تهدیدات محافظت می کند.

### اسپم تایتان چیست؟

اسپم تایتان یک راه حل امنیتی کامل ایمیل است که از تجارت شما، کارمندان شما و مشتریانانتان محافظت می کند.

اسپم تایتان راه حل فوق العاده ساده برای تنظیم و مدیریت ایمیل است و از جمله ویژگیهای آن می توان به مواردی مانند دقت ۹۹،۹۷٪ شناسایی هرنامه، مسدود کردن ویروس و بدافزار، کنترل احراز هویت، اسکن خروجی و همچنین ساختارهای گزارشگری قوی، اشاره کرد.

### مشخصات محصول

#### فیلتر هرنامه

اسپم تایتان برای جلوگیری از دسترسی هرنامه به کاربران شما، ترافیک ایمیل سازمان شما را فیلتر می کند. این راه حل ۹۹،۹۷٪ تشخیص هرنامه را از طریق تجزیه و تحلیل هرنامه چند لایه که شامل موارد زیر است، تضمین می کند:



اسپم تایاتان با اسکن ایمیل‌های خروجی، از این امر جلوگیری می‌کند.

### احراز هویت

تنظیمات احراز هویت وب به شما امکان می‌دهد که در هر دامنه، بتوانید روش احراز هویتی که کاربر در ورود به سیستم استفاده کرده است را کنترل کنید. روش‌های احراز هویت زیر پشتیبانی می‌شوند:

داخلی (پیش فرض)، LDAP، SQL server، POP3 و IMAP

پشتیبانی از ماژول‌های احراز هویت خارجی تضمین می‌کند که زمانی که کاربران نمی‌خواهند چندین رمز عبور را به خاطر بسپارند. تمام تلاش‌های ورود، به سرور احراز هویت مناسب برای آن دامنه منتقل خواهد شد.

### مدیریت قرنطینه:

SpamTitan برای کاربر نهایی و مدیر شبکه امکان مدیریت اسپم‌ها را فراهم می‌کند.

**درباره Titan HQ:** TitanHQ یک شرکت ایرلندی فعال در حوزه امنیت می‌باشد که در سال ۱۹۹۹ تاسیس شده و امروز بیش از ۵۰۰۰ مشتری در بیش از ۱۲۰ کشور جهان دارد. اسپم تایتان، اولین محصول این شرکت بوده و یک آنتی اسپم فوق العاده قوی و برنده جوایز متعدد از سازمانهای جهانی است.



### رایان سامانه آرکا - نماینده انحصاری اسپم تایتان در ایران

تهران، خیابان شهید بهشتی، خیابان پاکستان، کوچه چهارم، پلاک ۱۱، طبقه چهارم، واحد ۷  
 آدرس: تهران، خیابان شهید بهشتی، خیابان پاکستان، کوچه چهارم، پلاک ۱۱، طبقه چهارم، واحد ۷  
 تلفن: ۸۸۸۰۴۹۶۱ | دورنگار: ۸۹۷۸۳۷۳۷ | کدپستی: ۱۵۳۱۶۴۵۹۱۸  
 رایان سامانه آرکا | info@arka.ir | www.arka.ir

کلیه حقوق مادی و معنوی محفوظ و متعلق به شرکت رایان سامانه آرکا می‌باشد.

لیست‌های سیاه در زمان واقعی (RBL)، لیست وب سایت‌هایی که در ایمیل‌های ناخواسته شناسایی شده‌اند (SURBL)، چارچوب‌های سیاست فرستنده و تجزیه و تحلیل بی‌زی.

این موارد همراه با نرخ مثبت کاذب کم ۰.۳٪ به شما امکان می‌دهد خیالتان راحت باشد زیرا کاربران هرگز ایمیل اصلی را از دست نمی‌دهند، اما در مقابل ایمیل‌های ناخواسته محافظت می‌شوند.

### مسدود کردن ویروس و بدافزار

استفاده از دو موتور ضد ویروس Bitdefender و ClamAV که برای مسدود کردن ویروس‌ها و بدافزارها که در تلاش برای نفوذ به شبکه شما از طریق ایمیل هستند، راه حلی اثبات شده و موثر است.

### لیست سفید/لیست سیاه

این راه حل به شما امکان می‌دهد آدرس‌های ایمیل فرستنده را در لیست سفید / لیست سیاه قرار دهید، به این معنی که می‌توانید انتخاب کنید که نامه‌ها را همیشه از طریق یک آدرس ایمیل خاص مسدود یا قبول کنید.

### گزارش دهی و تایید گیرنده

اسپم تایتان می‌تواند گزارش‌های قرنطینه‌ای را در زمان‌ها و فواصل مشخص برای کاربران ارسال کند. گزارش قرنطینه شامل لیستی از ایمیل‌هایی است که برای کاربر ارسال نشده است زیرا به طور بالقوه حاوی اسپم یا ویروس است. کاربر نهایی می‌تواند تصمیم بگیرد ایمیل‌های موجود در گزارش قرنطینه را تحویل، لیست سفید و یا حذف کند.

### اسکن ایمیل‌های خروجی

امروزه اسکن ایمیل‌های خروجی از ایمیل سرور بسیار حیاتی است. این امر از ارسال هرزنامه و ویروس‌ها از سازمان شما جلوگیری می‌کند، بنابراین از قرار گرفتن IP‌های شما در لیست سیاه به عنوان اسپمر توسط یکی از سرویس‌های لیست سیاه جهانی جلوگیری می‌کند.

در صورتیکه ایمیل سرور شما در لیست سیاه قرار بگیرد، ارسال ایمیل مختل شده و تقریباً به هیچ‌جا ایمیل ارسال نمی‌شود. خارج کردن IP از لیست سیاه امری وقت‌گیر و سخت است.