Bitdefender

راهنمای مقاوم‌سازی سامانه امنیت نقاط پایانی بیت‌دیفندر

بر اساس توصیه‌نامه مرکز ماهر

شبکه گستر

امنیت شما | وظیفه ما

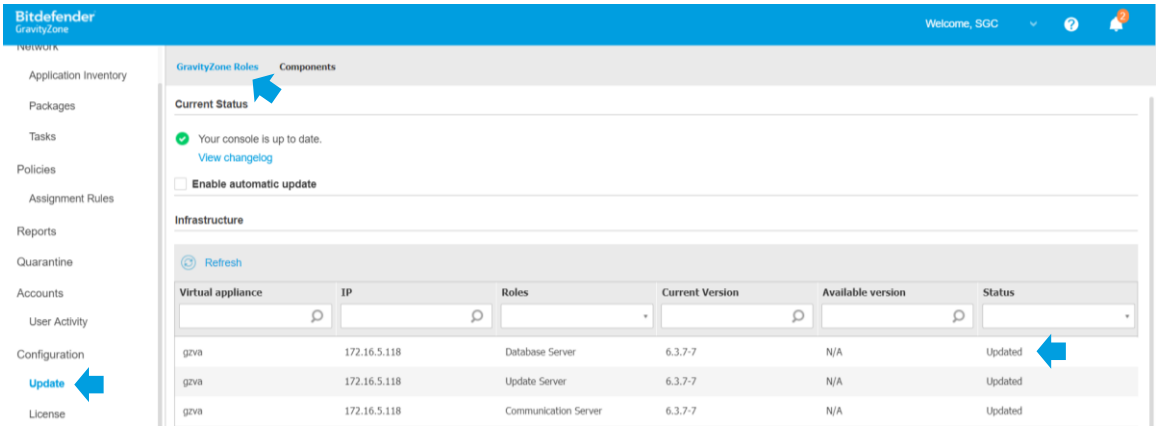
مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور (ماهر) توصیه‌نامه‌ای برای امن‌سازی سامانه‌های فناوری اطلاعات در مقابل تهدیدات سایبری احتمالی همزمان با ۱۳ آبان ماه منتشر کرده که در آن طی ۱۰ بند مواردی جهت مقاوم‌سازی سامانه‌ها ارائه شده است.

شرکت مهندسی شبکه گستر هم‌راستا با توصیه‌نامه فوق اقدام به انتشار راهنمای مقاوم‌سازی محصولات خود مطابق با بندهای مورد اشاره مرکز ماهر کرده است.

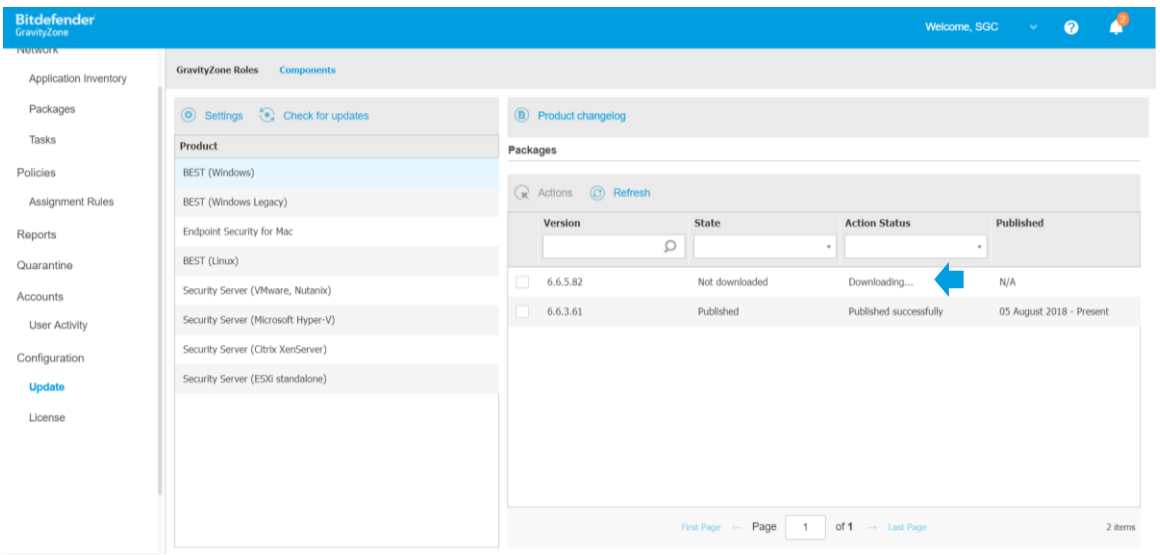
در این راهنما نحوه بررسی تنظیمات سامانه امنیت نقاط پایانی بیت‌دیفندر در جهت اجرای توصیه‌های مرکز ماهر ارائه گردیده است.

به‌روزرسانی سیستم عامل و نرم‌افزارها

امکان به‌روزرسانی هسته سیستم عامل سرور و نسخه نرم‌افزاری محصولات سازمانی بیت‌دیفندر در کنسول مدیریتی GravityZone فراهم است. جهت بررسی نسخه، باید در کنسول مذکور به بخش Configuration | Update مراجعه کرده و هر دو سربرگ GravityZone Roles و Components را مورد بازبینی قرار داد.



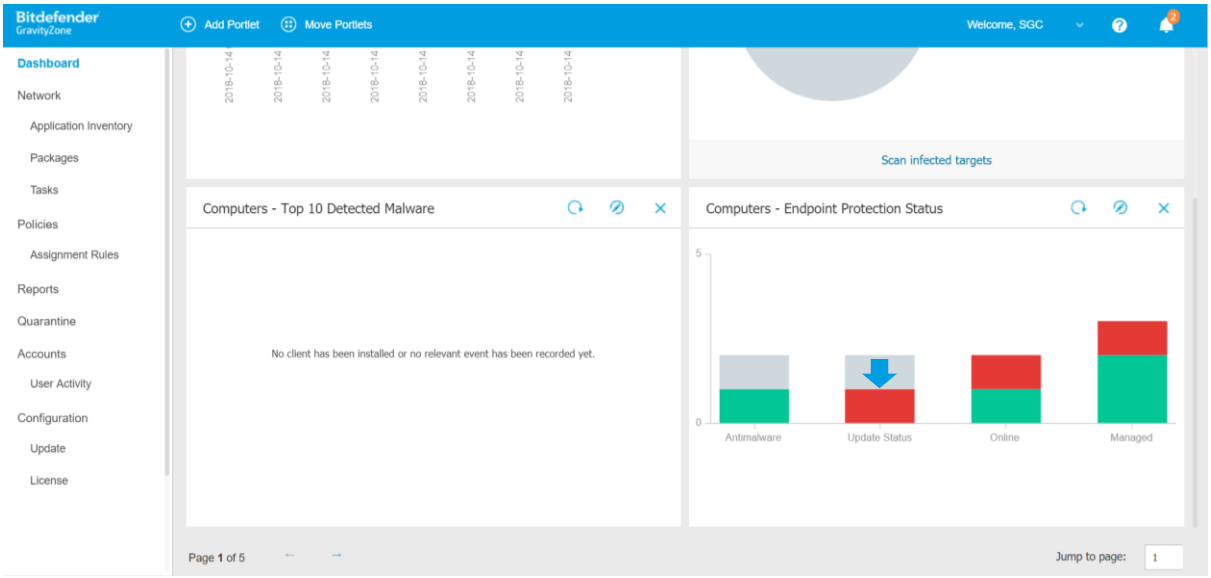
شکل ۱: وضعیت به‌روزرسانی اجزای ابزار مدیریتی GravityZone



شکل ۲: وضعیت به‌روزرسانی نرم‌افزارهای قابل توزیع در سطح شبکه توسط ابزار مدیریتی GravityZone

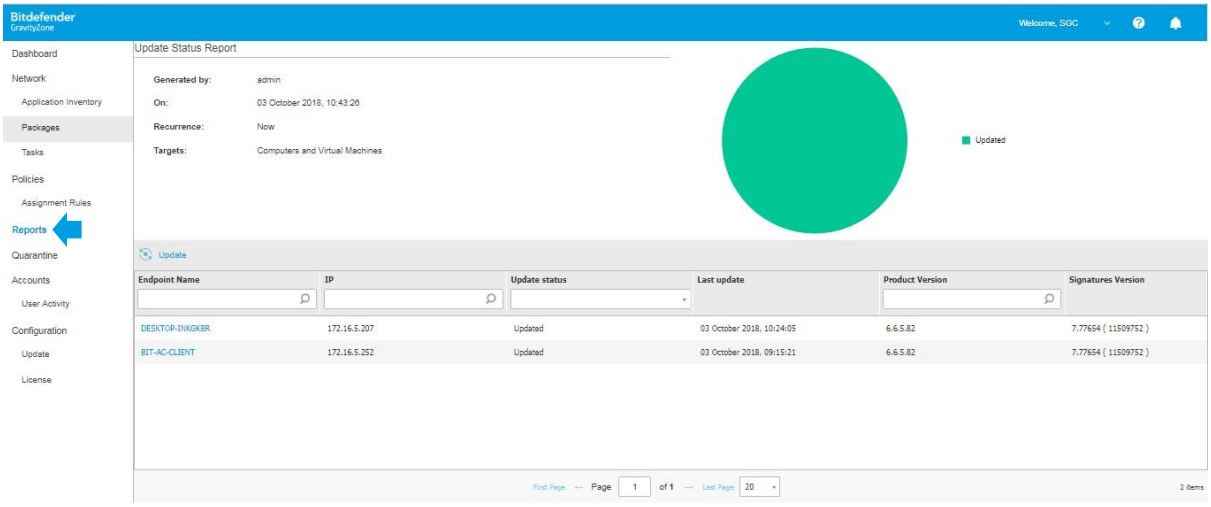
به‌منظور جلوگیری از وجود هرگونه نقطه ضعف امنیتی بر روی سرور مدیریتی و همچنین بسته‌های نرم‌افزاری نصب شده بر روی دستگاه‌های تحت پوشش، نصب به‌روزرسانی‌ها در اولین فرصت ممکن توصیه می‌شود.

همچنین جهت بررسی وضعیت به‌روزرسانی دستگاه‌ها و ماشین‌های تحت پوشش GravityZone می‌توان از نماهای Endpoint Protection Status در بخش Dashboard ابزار مدیریتی استفاده کرد.



شکل ۳: وضعیت به‌روزرسانی ضدویروس دستگاه‌ها و ماشین‌های تحت پوشش GravityZone (فلش آبی رنگ)

این جزییات در گزارش Update Status در بخش Reports نیز قابل مشاهده است.



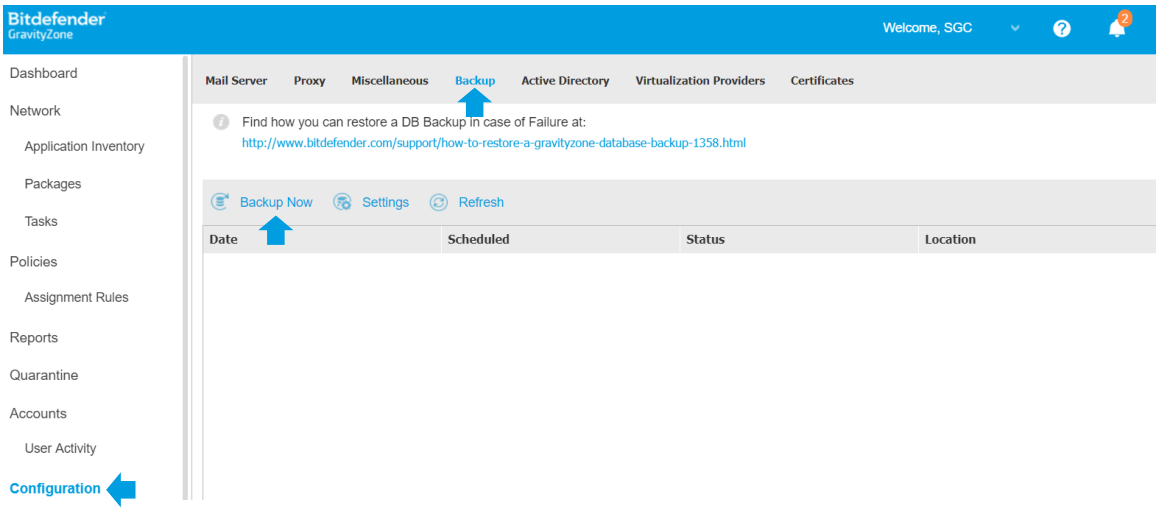
شکل ۴: گزارش Update Status در بخش Reports

در صورت عدم دریافت به‌روزرسانی توسط هر یک کامپیوترهای تحت پوشش این سامانه، پس از اطمینان از نکات زیر، موضوع از طریق شماره تلفن ۴۲۰۵۲ یا سامانه خدمات پس از فروش و پشتیبانی شرکت مهندسی شبکه گستر (MY) به نشانی https://my.shabakeh.net به گروه پشتیبانی شرکت مهندسی شبکه گستر اعلام شود:

- فراهم بودن ارتباط شبکه‌ای مناسب بین سرور GravityZone و کامپیوتر مورد نظر
- فراهم بودن حداقل فضای خالی بر روی دیسک سخت کامپیوتر مورد نظر

تهیه و نگهداری نسخه پشتیبان

با مراجعه به بخش Configuration | Backup در کنسول مدیریتی GravityZone می‌توان از پایگاه داده و تنظیمات سرور نسخه پشتیبان تهیه نموده و یا انجام آن را زمانبندی کرد.



شکل ۵: بخش Backup در ابزار مدیریتی GravityZone

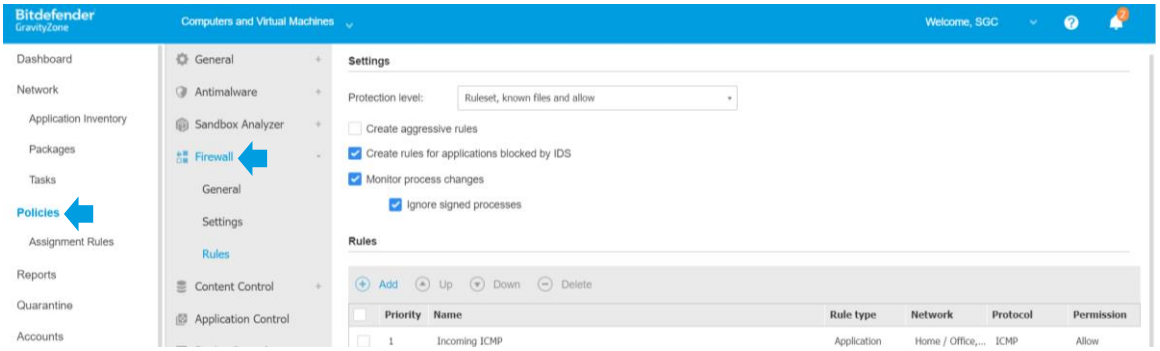
همچنین با استفاده از راهنمای ساخت تصویر لحظه‌ای از ماشین GravityZone در سامانه MY می‌توان در بستر مجازی‌سازی اقدام به تهیه نسخه پشتیبان کرد.

بهره‌گیری از رمزنگاری مناسب در تبادل اطلاعات

ارتباطات میان دستگاه‌ها و ماشین‌ها با سرور GravityZone از طریق پودمان امن HTTPS برقرار می‌گردد.

اتخاذ راه‌حل برای دسترسی ایمن از راه دور برای مدیریت سرویس‌ها و زیرساخت‌ها

اگر چه تلاش گردیده که حداکثر مقاوم‌سازی ممکن بر روی ماشین(های) مجازی GravityZone اعمال شود اما کنترل دسترسی به آن از طریق استفاده از دیواره آتش توصیه می‌گردد. ضمن اینکه در بخش Policies | Firewall در کنسول مدیریتی GravityZone امکان اعمال قواعد متنوع دیواره آتش بر روی دستگاه‌های تحت پوشش فراهم می‌باشد.



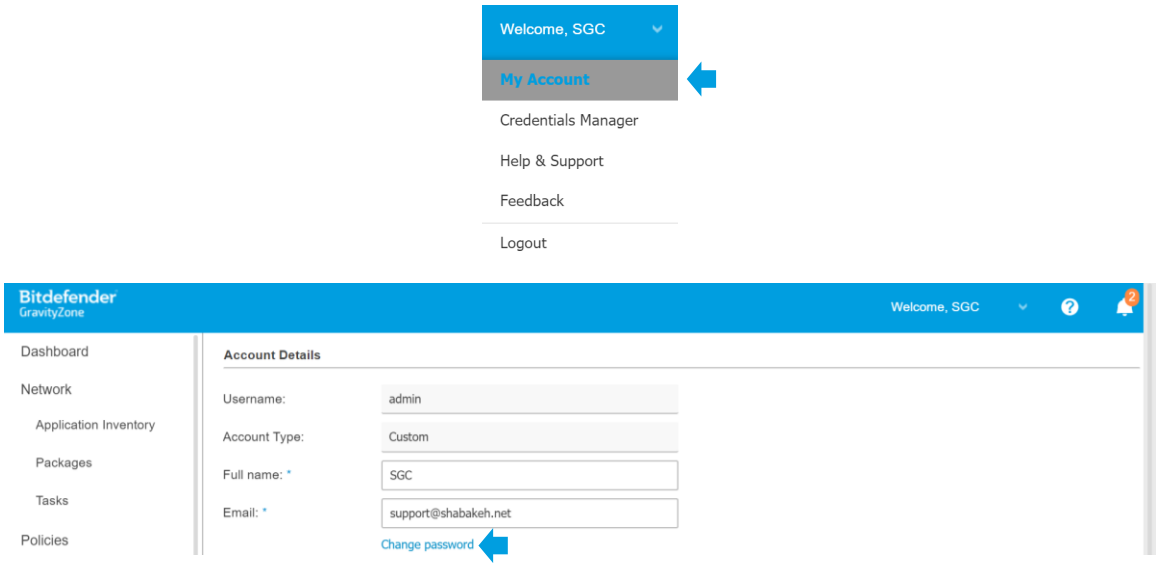
شکل ۶: قواعد دیواره آتش در ابزار مدیریتی GravityZone

اتخاذ مکانیزم احراز هویت و رمز عبور قوی

توصیه می‌شود تمامی رمزهای عبور، پیچیده[1] و حاوی بیش از ۱۰ نویسه[2] باشند.

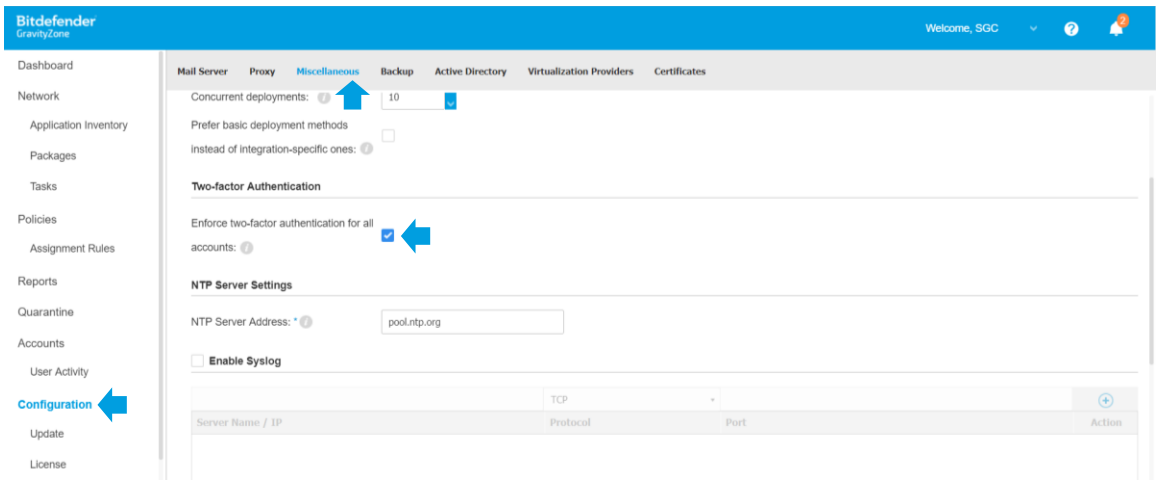
سیستم عامل مورد استفاده در راهکار GravityZone دارای کاربری با سطح دسترسی root با نام bdadmin است که نحوه تغییر رمز عبور آن در راهنمای تغییر رمز عبور سیستم عامل و کنسول Bitdefender GravityZone بر روی سامانه MY قابل مطالعه است.

همچنین در کنسول مدیریتی GravityZone با کلیک بر روی نام کاربری و انتخاب گزینه My Account می‌توان رمز عبور کاربر جاری را تغییر داد.



شکل ۷: تغییر رمز عبور کاربر جاری

با مراجعه به بخش Configuration | Miscellaneous و فعال کردن گزینه Enforce two-factor authentication for all accounts نیز می‌توان قابلیت اصالت‌سنجی دو مرحله‌ای را برای کلیه نام‌های کاربری دارای دسترسی به GravityZone فعال کرد.



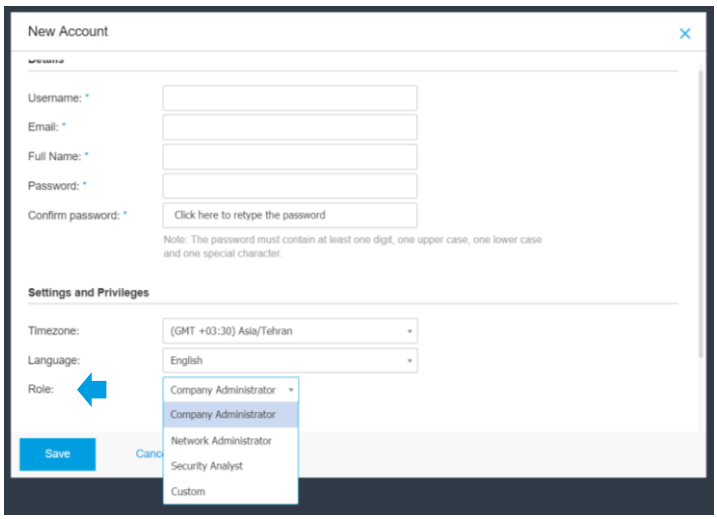
شکل ۸: نحوه فعالسازی اصالت‌سنجی دومرحله‌ای

---

[1] Complex Password

[2] Character

GravityZone امکان تعریف هر تعداد راهبر با سطوح دسترسی متفاوت را فراهم می‌کند. توصیه می‌شود که به هر یک از این راهبران دسترسی مناسب – در حداقل سطح ممکن – تعریف شود. برای این منظور می‌توان به بخش Accounts در کنسول مدیریتی GravityZone مراجعه کرد.

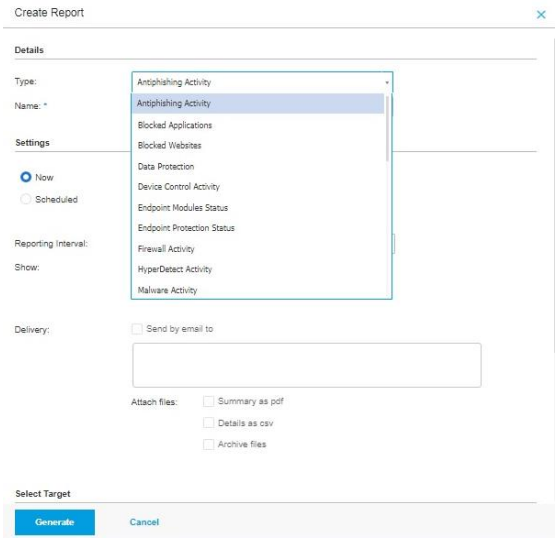


شکل ۹: تعریف کاربر جدید در ابزار مدیریتی GravityZone

همچنین در صورت استفاده از دامنه[۳] امکان ورود به کنسول مدیریتی GravityZone با نام کاربری مبتنی بر دامنه فراهم می‌باشد.

جمع‌آوری، نگهداری و بررسی رخدادنماها

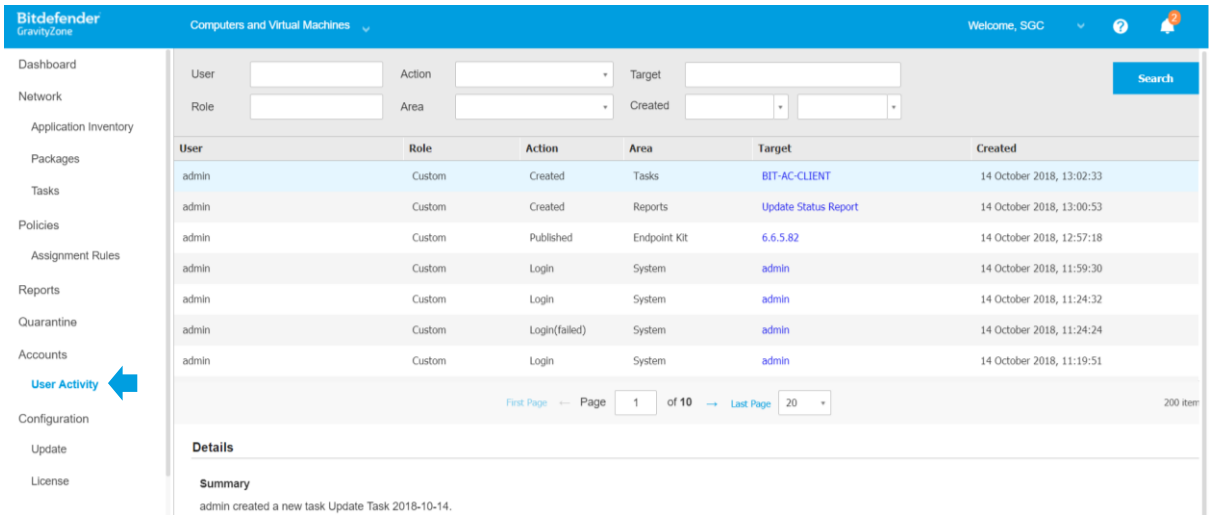
امکان گزارش‌گیری و رصد رخدادهای امنیتی صورت گرفته در سطح شبکه از طریق بخش Reports در ابزار مدیریتی GravityZone فراهم می باشد. خروجی این گزارش‌ها را می‌توان جهت مستندسازی در قالب‌های PDF و Excel ذخیره نمود.



شکل ۱۰: انواع گزارش‌ها در ابزار مدیریتی GravityZone

[۳] Domain

در مسیر Accounts | User Activity نیز فعالیت راهبران GravityZone قابل رصد است.

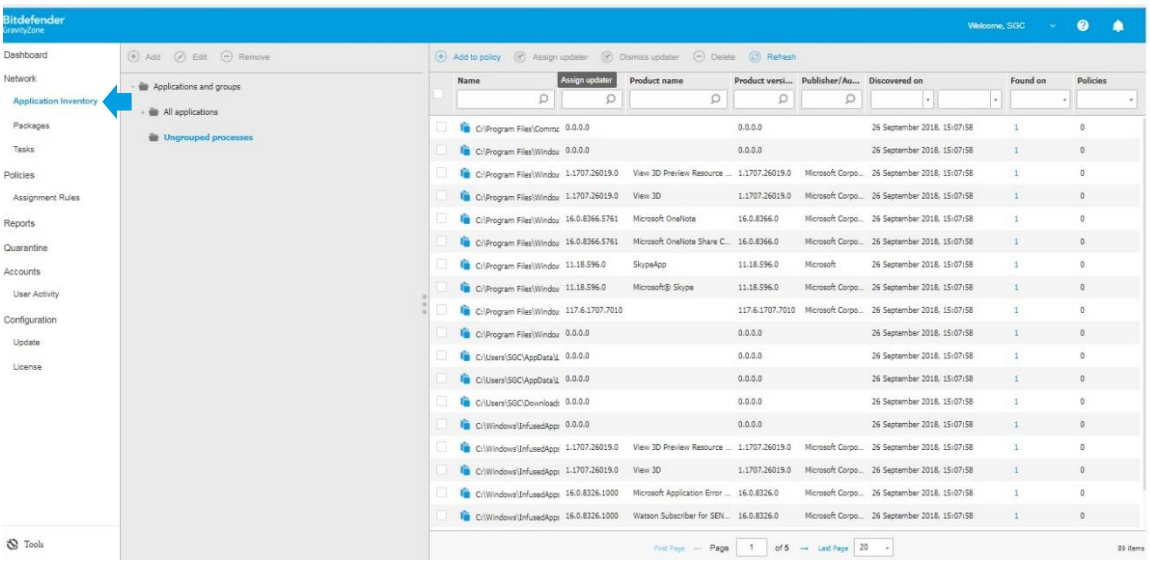


شکل ۱۱: سوابق فعالیت راهبران در کنسول مدیریتی GravityZone

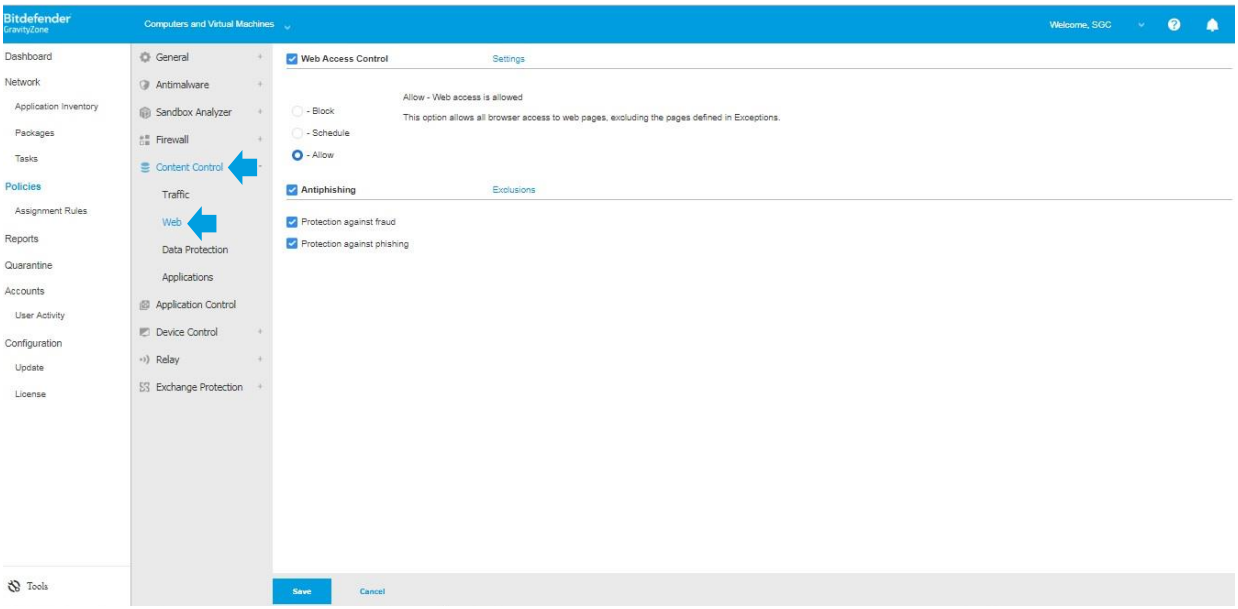
جلوگیری از نشت اطلاعات سازمانی

امکان کنترل و جلوگیری از دسترسی به درگاه‌های وب غیرمجاز بر اساس سیاست‌های سازمان - نظیر شبکه‌های اجتماعی - و یا اجرای نرم‌افزارهای خاص از طریق قابلیت‌های Content Control و یا Application Control فراهم می‌باشد.

برای مثال، می‌توان دسترسی کاربران موجود در سطح شبکه را به یک یا چند نشانی وب خاص محدود کرد و یا تنها اجازه استفاده از نرم‌افزارهای مورد تایید سازمان را بر روی ایستگاه‌های کاری موجود در شبکه صادر نمود.



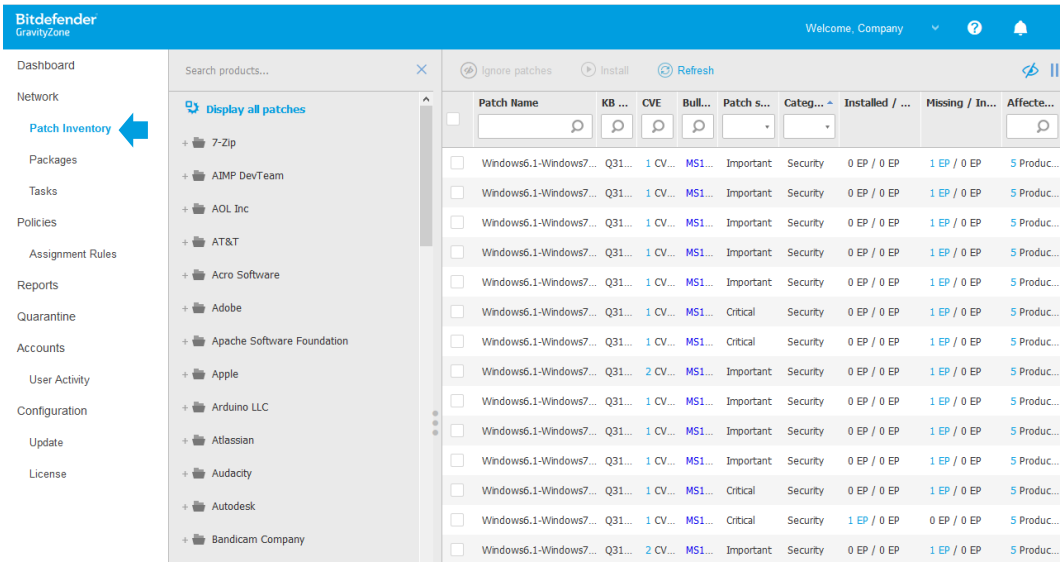
شکل ۱۲: انباره برنامه‌های شناسایی شده بر روی دستگاه های تحت پوشش



شکل ۱۳: بخش Web در تنظیمات Content Control

ترمیم آسیب‌پذیری‌ها

محصول Bitdefender Patch Management امکان به‌روزرسانی و نصب اصلاحیه‌های مربوط به سیستم عامل و نرم‌افزارهای نصب شده در سطح سازمان را فراهم می‌کند. این محصول فایل‌های به‌روزرسانی و اصلاحیه‌ها را بر روی دستگاه یا دستگاه‌های تعیین شده دریافت و به‌صورت متمرکز آنها را بر روی ماشین‌ها و دستگاه‌های تحت پوشش توزیع می‌کند.



شکل ۱۴: انباره اصلاحیه‌های امنیتی

درباره ما

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تاسیس شد. این شرکت یکی از باسابقه‌ترین شرکتهای فعال در حوزه امنیت فناوری اطلاعات است. با بیش از ۲۵ سال تجربه موفق در عرضه محصولات و خدمات امنیت شبکه، شرکت شبکه گستر افتخار خدمات‌دهی به هزاران شرکت و سازمان در بخش‌های مختلف کشور را دارد و مجری بزرگترین پروژه‌های نصب و نگهداری نرم‌افزارهای ضدبدافزار و سخت‌افزارهای دیـواره آتش در کشور بوده است.

شبکه گستر
شـرکـت مـهـنـدسـی شـبـکـه گـسـتـر

تهران خیابان شهید دستگردی (ظـفـر) شماره ۲۷۳
تلفن / دورنگار ۴۲۰۵۲ – ۰۲۱
info@shabakeh.net www.shabakeh.net

سناسه سند: SPT-E-0311-00