راهنمای نصب و کار با بسته امنیتی

این بسته امنیتی همواره از برترین ها در دنیای اینترنت است و به گواهی بیشتر منابع و مجلات معتبر دنیای فناوری اطلاعات، در مقایسه با سایر شرکت های معتبر امنیتی، جایگاه اول را در اختیار دارد. از لپ تاپ ها، کامپیوترهای رومیزی و سرورهای شبکه شما در برابر بدافزارها، خطرات و آسیب پذیری ها محافظت کرده و همزمان اجرای بسیار سبک، سرعت بالا و کارآیی آسان را در یک کامپیوتر به ارمغان می آورد.

فناوری پیشرفته سیمانتک، حفاظت در برابر ویروس را با امنیت نسبت به تهدید پیشرفته، ترکیب می کند

به نحوی که بطور فعال کامپیوتر شما را در برابر تهدیدات شناخته شده و ناشناخته مانند ویروس ها، کرم ها، اسب های تروجان و حملات جدید روزانه ایمن می سازد.

بسته امنیتی کامل در دو نسخه 32 بیت و 64 بیت برای سیستم عامل های Windows, Linux, MAC ارائه شده است. نسبت به سایر نرم افزار های امنیتی، بهترین همخوانی را با سیستم عامل ویندوز داشته و بطور خودکار فایروال ویندوز تحت کنترل بسته امنیتی قرار می گیرد.

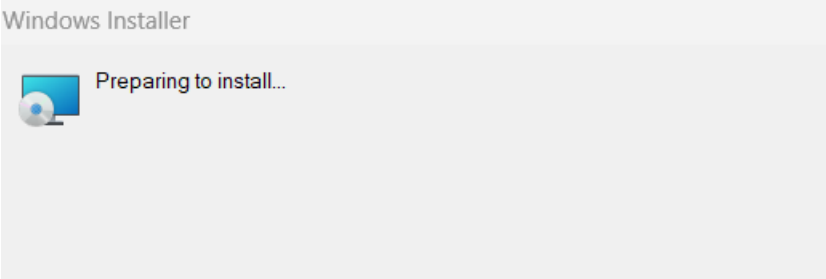
لطفا قبل از نصب در صورت داشتن هرگونه آنتی ویروس ، آن را از روی سیستم حذف کرده و سیستم را دوباره راه اندازی نمایید. سپس با توجه به نوع سیستم عامل خود ، می توانید بر روی فایل setup بسته امنیتی دوبار کلیک نمایید تا فرآیند نصب آغاز شود.

WIN64BIT

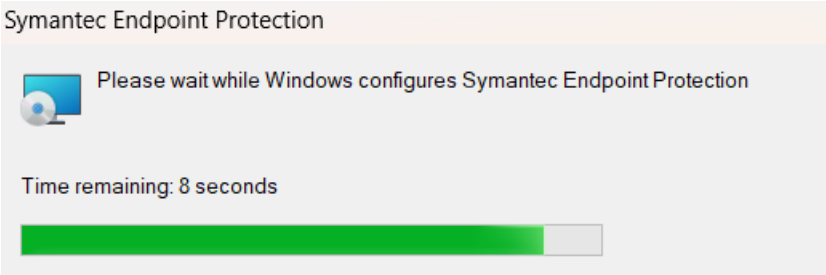
WIN32BIT

در برخی سیستم عامل ها که به روز رسانی نشده اند، ممکن است از شما درخواست نصب فایل به روز رسانی ویندوز را نماید. در اینصورت، با کلیک بر روی لینک نمایش داده شده و سپس دانلود نسخه مورد نیاز فایل به روز رسانی از سایت مایکروسافت، می توانید آن را نصب نمایید.

سپس ویندوز را مجدد راه اندازی و بسته امنیتی را نصب نمایید



لطفا صبر نمایید تا مراحل نصب بصورت خودکار انجام شود.



در انتهای مراحل نصب، پنجره کادر ثبت محصول ظاهر می شود.

در پایان، پنجره کادر ثبت محصول ظاهر می شود.

حال مشخصات خود را وارد نمایید. مشخصات خریدار شامل موارد زیر است:

- نام و نام خانوادگی (فارسی)
- ایمیل
- شماره سریال خریداری شده
- شماره موبایل

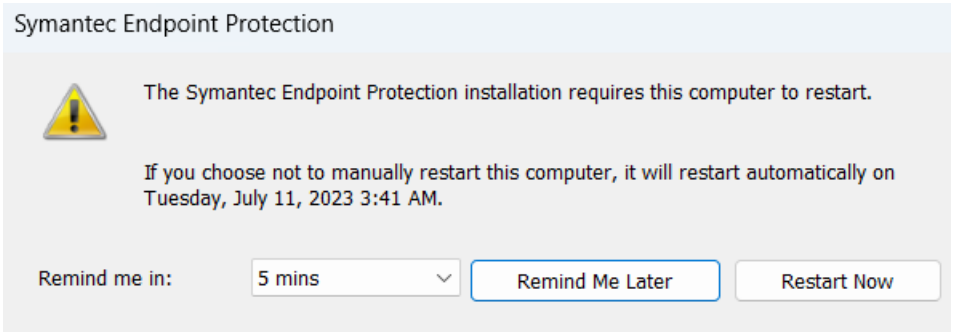
در صورتیکه بسته امنیتی را بصورت آزمایشی نصب می کنید، **5555** را در کادر شماره سریال وارد نمایید.

در صورتیکه کد معرف دارید، آن را در کادر مربوطه وارد نمایید.

موارد فوق را بصورت دقیق وارد نمایید تا فرآیند ثبت محصول خریداری شده، بصورت کامل انجام شود.

این اطلاعات و شماره تراکنش خرید محصول، جهت پشتیبانی محصول ضروری است.

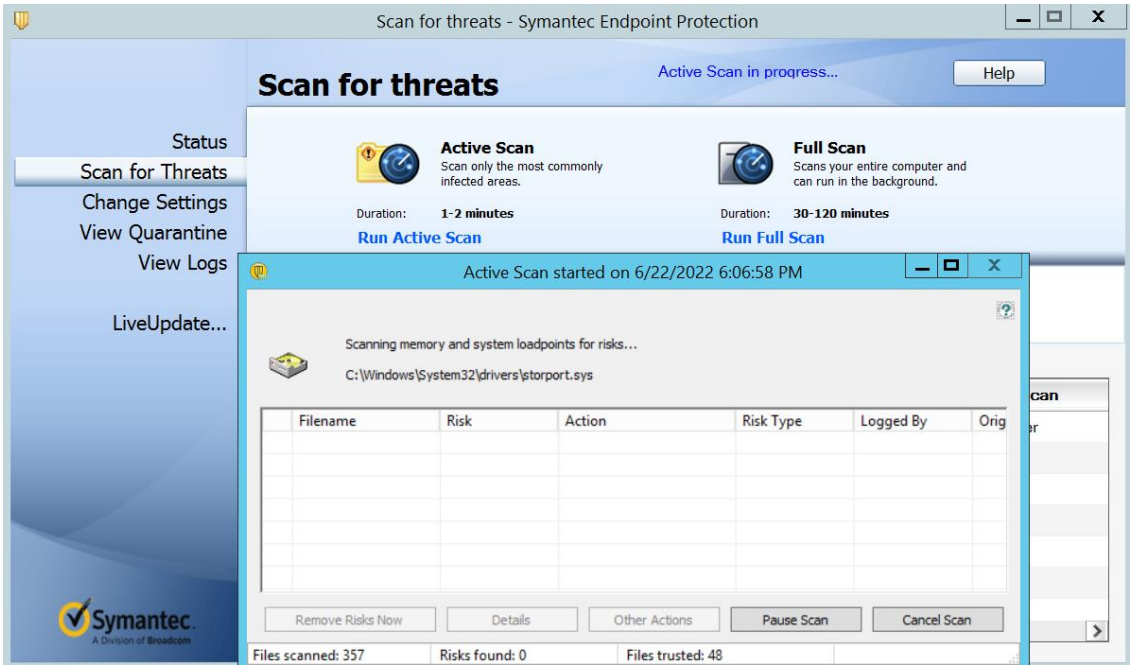
سپس در پنجره نهایی، با کلیک بر روی **Restart Now**، اجازه دهید تا نصب بصورت کامل انجام شود.



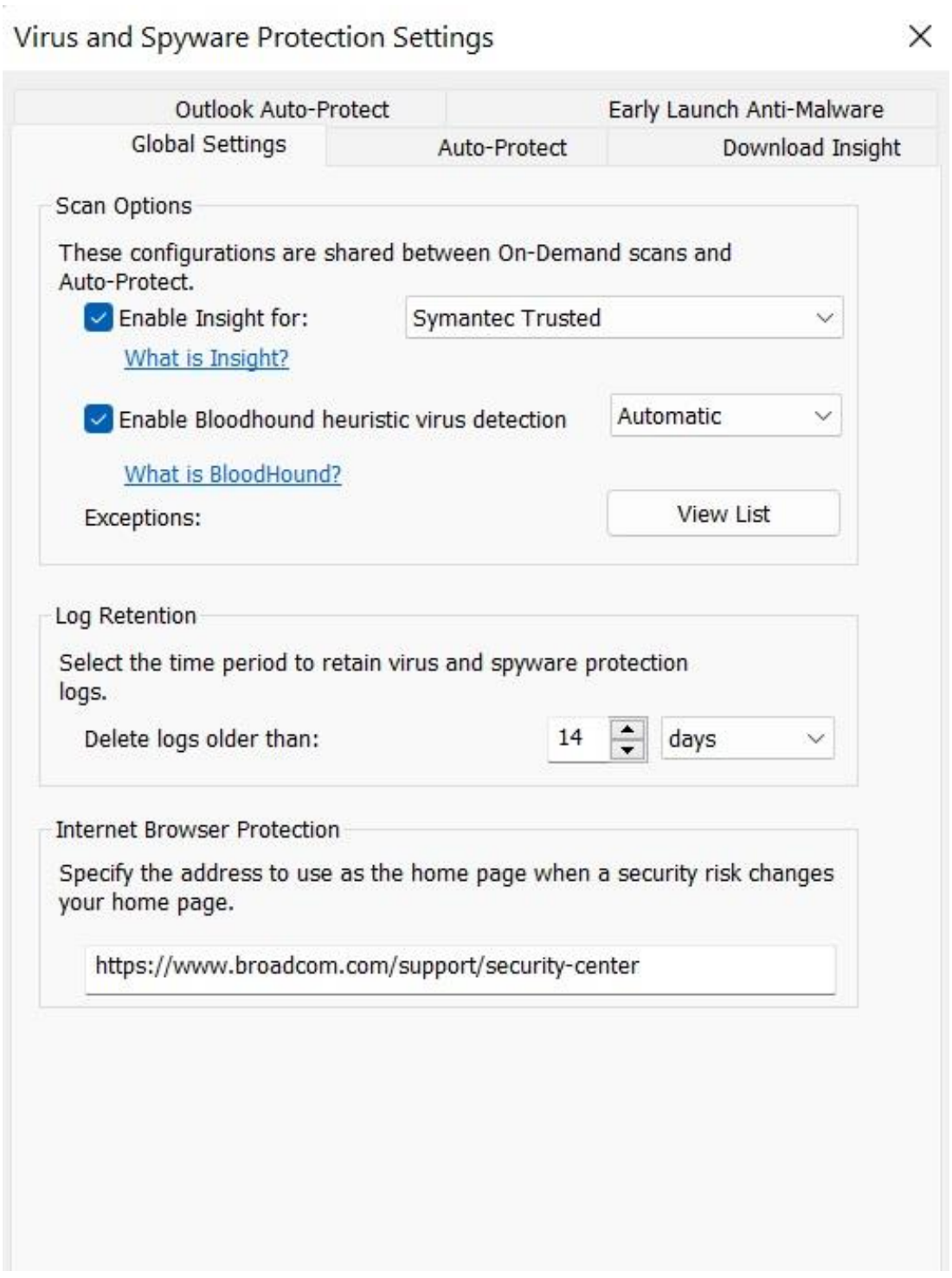
پس از راه اندازی ویندوز **Symantec Endpoint Protection** بر روی کامپیوتر شما نصب شده است آن را اجرا نمایید. در کادر ظاهر شده ، کلمه عبور بسته امنیتی را وارد نمایید. سپس وارد محیط نرم افزار می شوید. مدت زمانی پس از خرید و ثبت کامل محصول ، کادر رمز عبور حذف خواهد شد.

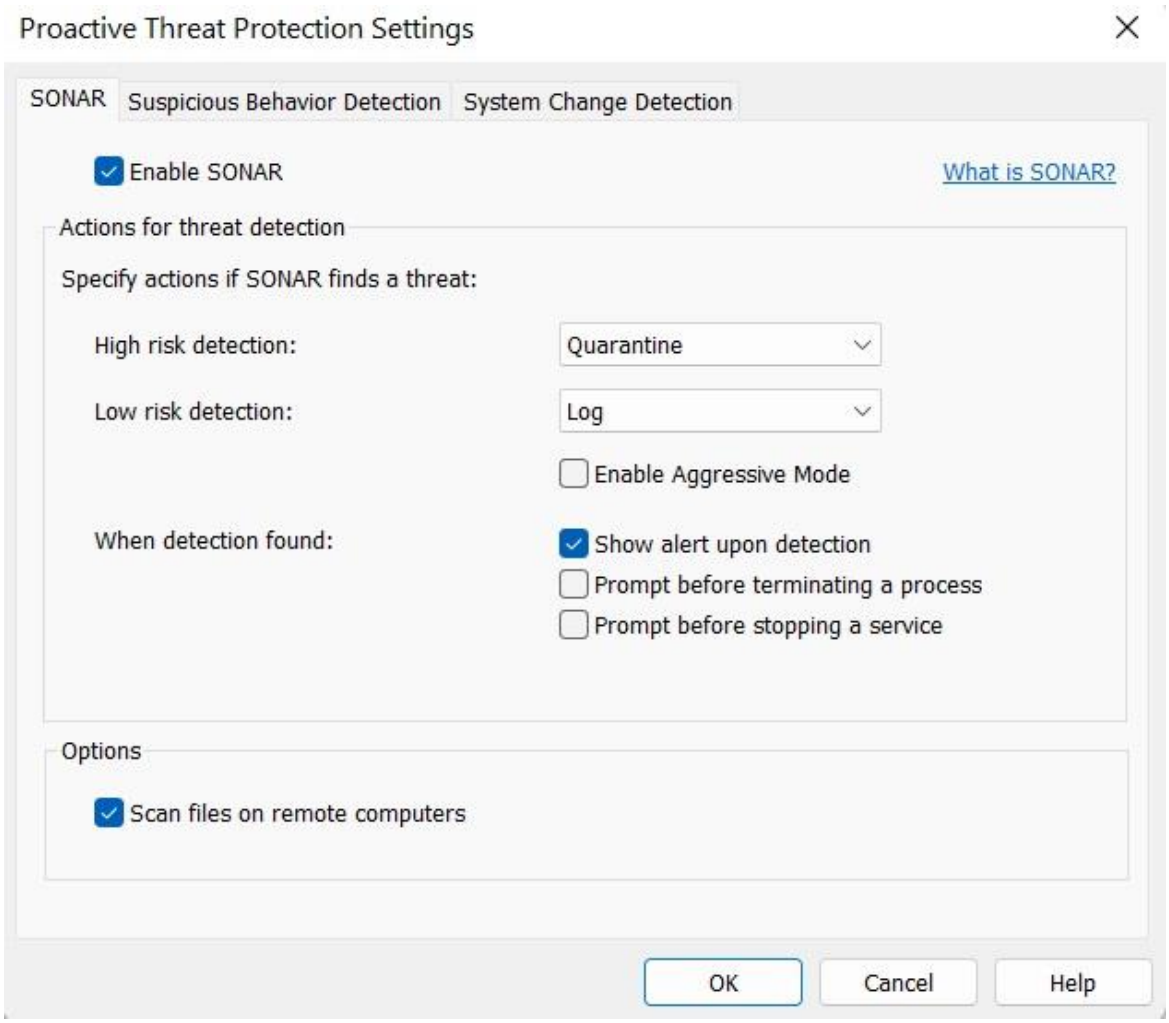
در صفحه اصلی، می توانید با کلیک بر روی **LiveUpdate** ، فرآیند به روز رسانی را انجام دهید . این کار همواره بطور خودکار انجام می شود.

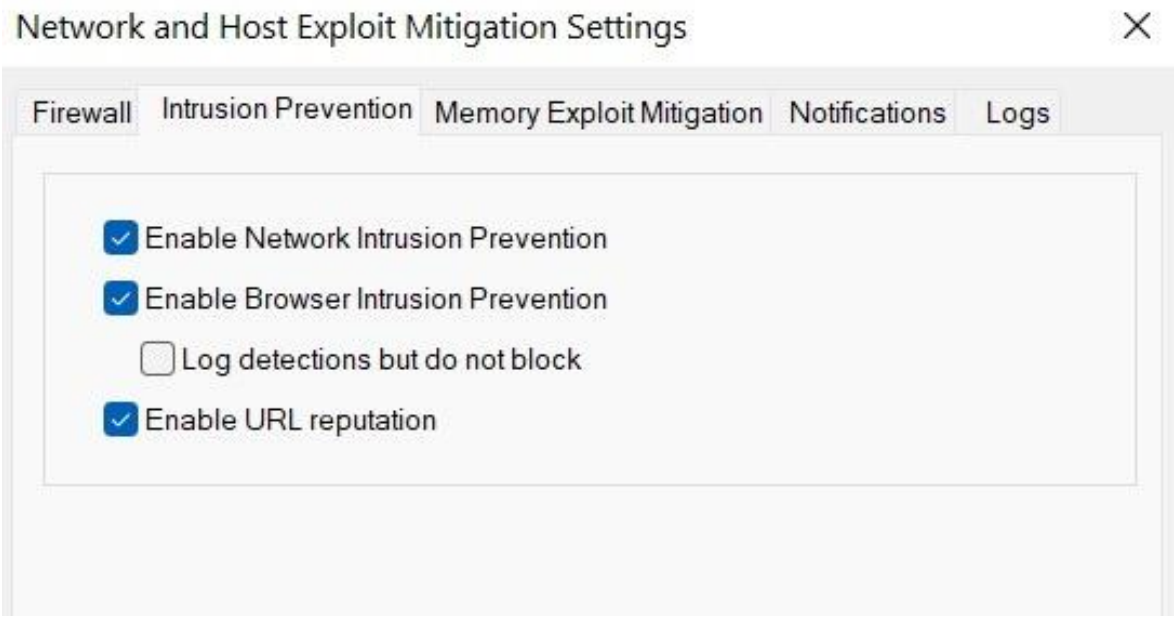
همچنین می توانید از قسمت **Scan for Threats** ، کامپیوتر خود را بصورت سریع و یا کامل اسکن نمایید.



بسته امنیتی دارای قسمت های پیشرفته تنظیمات می باشد و تمامی موارد فعالیت آن بصورت پیش فرض انجام می شود.



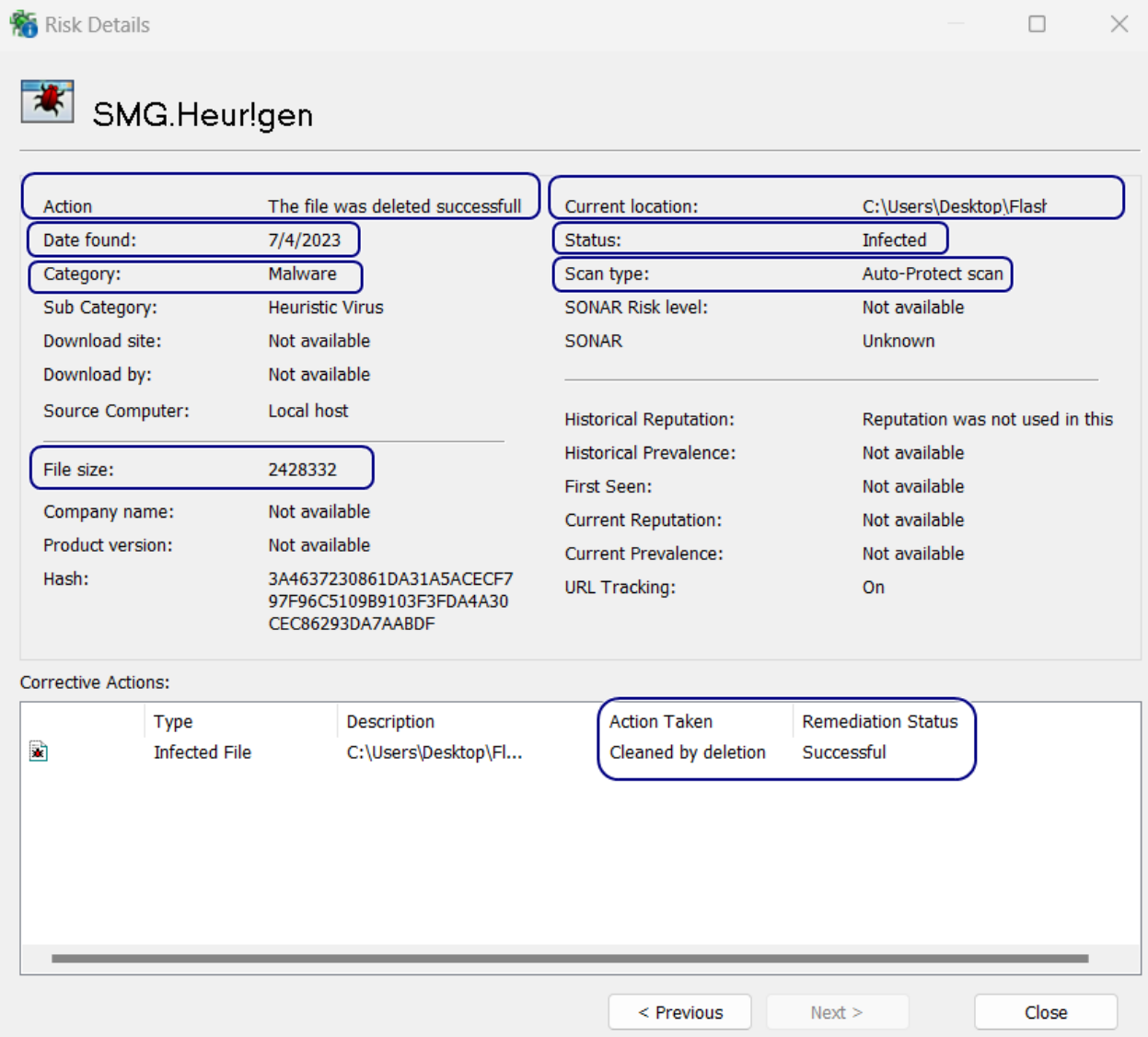

Proactive Threat Protection Settings
SONAR
Suspicious Behavior Detection
System Change Detection
Enable SONAR
What is SONAR?
Actions for threat detection
Specify actions if SONAR finds a threat:
High risk detection:
Quarantine
Low risk detection:
Log
Enable Aggressive Mode
When detection found:
Show alert upon detection
Prompt before terminating a process
Prompt before stopping a service
Options
Scan files on remote computers
OK
Cancel
Help


Network and Host Exploit Mitigation Settings
Firewall
Intrusion Prevention
Memory Exploit Mitigation
Notifications
Logs
Enable Network Intrusion Prevention
Enable Browser Intrusion Prevention
Log detections but do not block
Enable URL reputation

در صورت وجود هرگونه ویروس و خطرات امنیتی ، می توانید در بخش **View Quarantine** ، لیست آنها را مشاهده نمایید.

با راست کلیک کردن بر روی یک فایل قرنطینه شده، می توانید موارد زیر را انجام دهید:

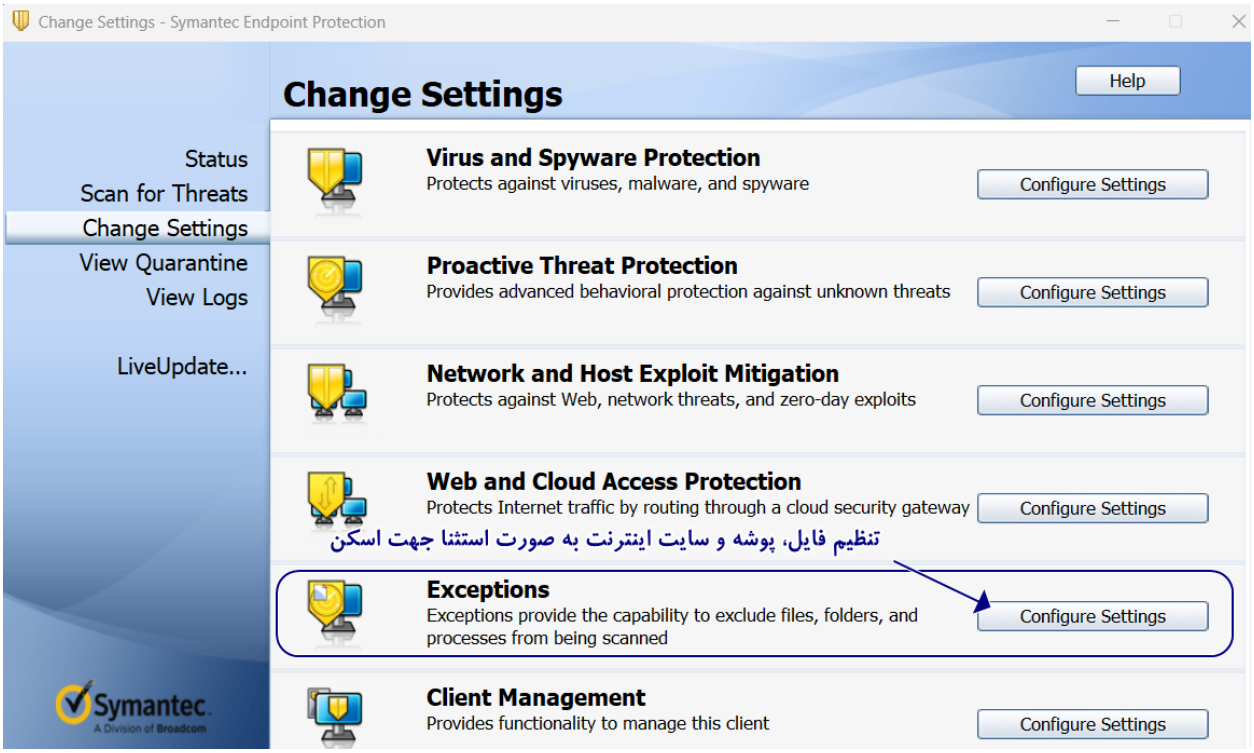
- در صورتیکه فکر می کنید فایلی به اشتباه قرنطینه شده است ، می توانید با کلیک بر روی گزینه **Restore** آن را به مکان اصلی خود باز یابی کنید.
- حتی در صورتیکه فایل مکانی نداشته باشد، مانند یک پیوست آلوده ایمیل که حذف شده و در قرنطینه قرار گرفته است، می توانید یک مکان برای آن در نظر بگیرید.
- همچنین با کلیک بر روی گزینه **Delete** می توانید فایل قرنطینه شده را بطور کامل حذف نمایید. به طور پیش فرض فایلهای قرنطینه شده هر **30** روز یکبار پاک می شوند.
- با کلیک بر روی گزینه **Properties** می توانید مشخصات تهدید امنیتی شامل، فعالیت انجام شده ، نوع ریسک تاریخ و مکان تهدید امنیتی را مشاهده نمایید.



راهنمای اعتماد سازی فایل، پوشه و سایت اینترنت

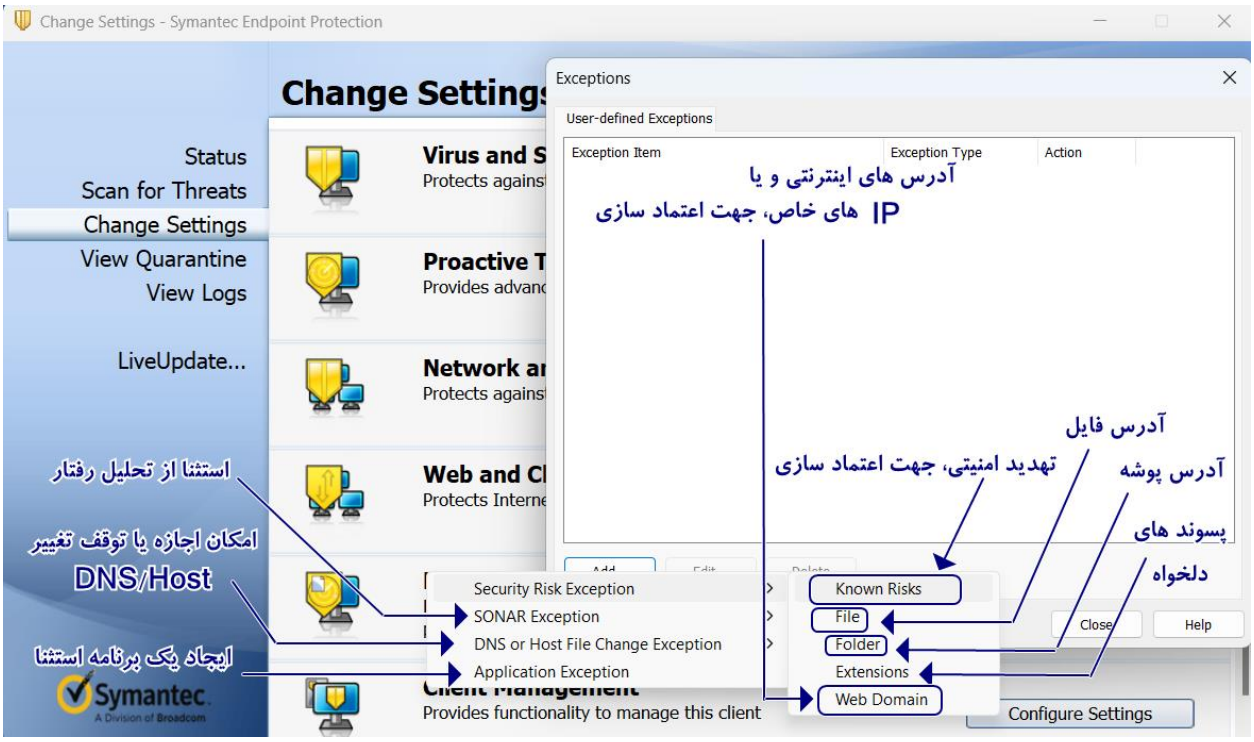
در صورت نیاز، می توانید از این بخش برای جدا کردن فایلها، پوشه ها، ریسک ها و فرآیندها از عملیات اسکن استفاده کنید (عدم اسکن). به عنوان مثال، ممکن است بخواهید فایل ها و یا پوشه هایی را تمایل دارید اسکن نشوند را در این کادر به عنوان موارد امن معرفی کنید ، نظیر کرک بازی های کامپیوتری که با اسکن کردن ممکن است به عنوان ویروس شناسایی شوند.

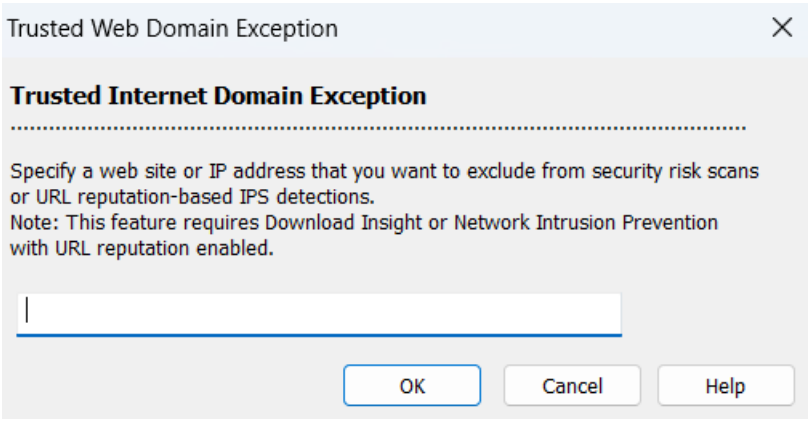
برای انجام این کار، در صفحه اصلی بر روی Settings Change کلیک نمایید . سپس در صفحه باز شده و قسمت Exceptions بر روی دکمه Configure Settings کلیک نمایید.



در صفحه باز شده بر روی دکمه **Add** کلیک نمایید.

همانطور که در تصویر نشان داده شده است، می توانید به تعداد دلخواه آدرس فایل، پوشه و سایت اینترنت را جهت اعتماد سازی به منظور عدم انجام اسکن توسط نرم افزار وارد نمایید.

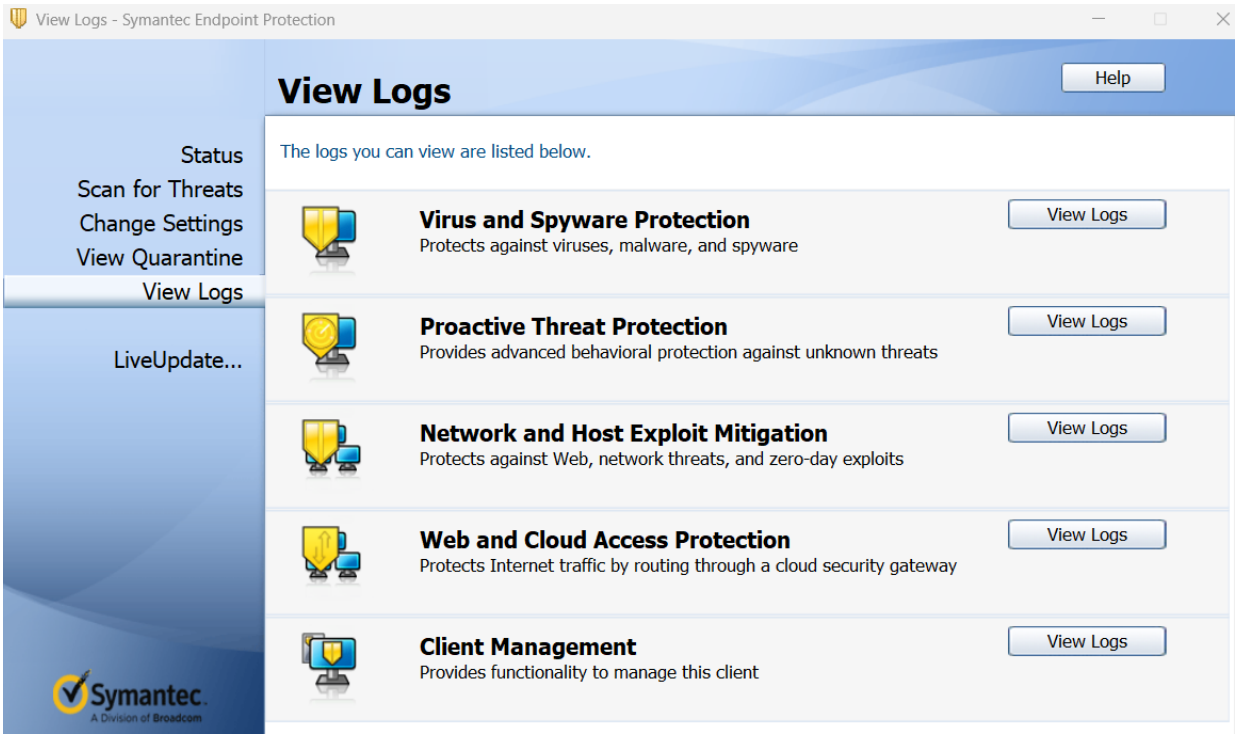


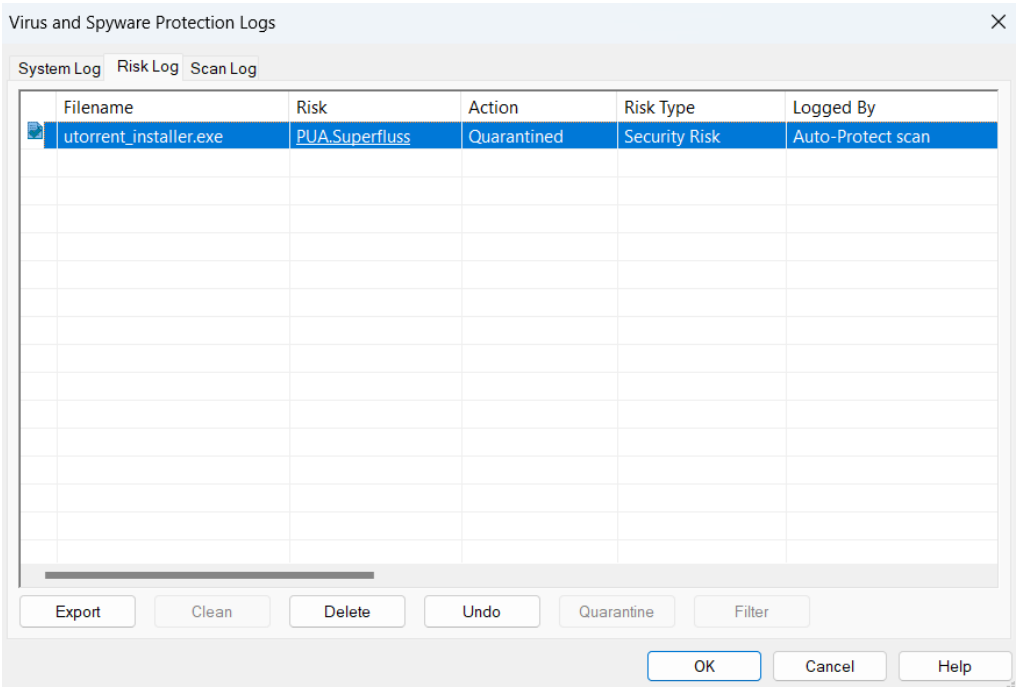


به عنوان مثال در قسمت
Web Domain
می توانید آدرس وب سایت ها و یا آدرس آی پی هایی که تمایل دارید در عملیات اسکن بسته امنیتی شرکت داده نشوند را وارد نمایید.

مشاهده گزارشات بخش های مختلف

در صفحه اصلی، بخش **View Logs** همواره می توانید گزارش قسمت های مختلف را مشاهده نمایید.





بسته امنیتی گزارش سوابق، تهدیدات، اسکن ها، تاریخ فعالیت ها و سایر جزئیات را بطور کامل در بخش های مختلف تقسیم بندی کرده و به شما نمایش می دهد.

نکته: لطفا جهت امنیت کامل و استفاده از تخفیف سالانه همواره اقدام به تمدید محصول نمایید.