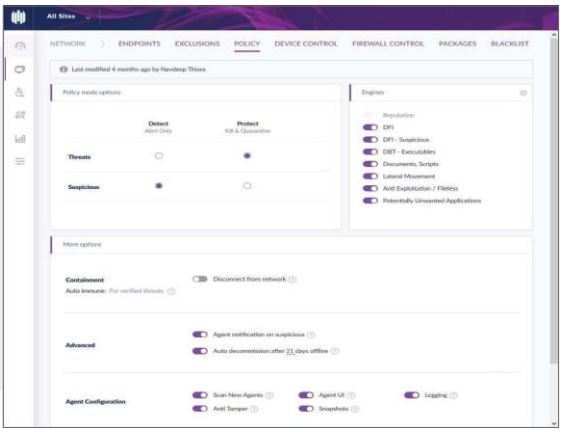
Remote User / Home User Security:

Corporate level threat protection for the home-based remote user

In response to the increase of Work from Home remote users, this product is designed to give the user-owned home-based PC the same level of threat protection provided in most corporate environments. Work safely at home knowing your PC is protected from the latest threats, malware, and encryption attacks. Packages start at $50 per PC.



PREVENT CYBERATTACKS

- ✓ Near real-time file analysis: The system can analyze files continuously, replacing time-intensive recurring scans.
- ✓ Signatureless approach: Fight back against the latest threats without having to wait for daily definition updates.
- ✓ Offline protection: Artificial intelligence data is stored on the endpoint to keep it protected while offline—and to help you avoid waiting for signature updates or waiting for the endpoint to connect to the cloud to check against reputation scores.

DETECT THREATS WITH BEHAVIORAL AI

- ✓ Behavioral artificial intelligence engines: The feature includes eight AI engines that analyze multiple data points to identify threats and determine if a response is necessary.
- ✓ Near real-time alerts: Discover threat activity quickly with alerts whenever a threat is detected or neutralized.
- ✓ Forensics: See an overview and the storyline of an attack, so you can quickly understand the threat.
- ✓ Threat summaries: Review information on specific threats, such as dates they were identified, dates they were reported, and their file names. Summaries also include links to the Google threat database and Virus Total websites for more information.

RESPOND EFFECTIVELY THROUGH AUTOMATION

- ✓ Custom policies: Use policy-driven protection tailored to your customer, which allows/blocks USB, allows/blocks endpoint traffic, and specifies the best automated response.
- ✓ Multiple recovery options: Choose your preferred recovery option after attacks—from partial recoveries to fully-automated responses.
- ✓ Enhanced quarantine: Select the Disconnect from Network option to prevent machines from further infecting the network.
- ✓ Automatic rollback: Attacks are automatically contained, and neutralized, and compromised files are automatically replaced by the last known healthy version.

WINDOWS AND 3RD PARTY PATCH MANAGEMENT AND INSTALLATION

- ✓ With patch management services, we ensure that all the necessary updates are being installed promptly. Patching includes many of the more commonly found software on PCs today such as Adobe Reader, Java, and other 3rd party software and applications. Patches are approved within our system and then released to workstations and servers on a scheduled basis.

WEB PROTECTION AND FILTERING

- ✓ This background service helps protect the user from accessing potentially harmful websites which may infect their PC with malware, spyware, and viruses, or spy on the user's activity. We block a full array of sites from pornography to social media and other questionable sites.

OPTIONAL: OFFICE 365 DATA PROTECTION INCLUDING EMAIL AND ONEDRIVE