Commented [MM1]: I'm using 2020 here, since we won't update this again until next version. Is this OK?
Trend Micro Incorporated reserves the right to make changes to this document and to the service described herein without notice. Before implementing the service, please review the readme file and the latest version of the applicable user documentation.

Copyright © 2019 Trend Micro Inc., Consumer Technical Product Marketing. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and Trend Micro Security are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners. Android is a trademark of Google, Inc. Mac is a trademark of Apple, Inc.


DOCUMENT PROFILE:
Document Title: Trend Micro™ Home Network Security 2020 - Product Guide
Document Release Date: October 3, 2019
Team: Consumer Technical Product Marketing
# Table of Contents

**Executive Summary** .................................................................................................................. 5  
Trend Micro Home Network Security Highlights ............................................................................. 6  

**Section 1: Detailed Product Specifications** .................................................................................. 8  
Key Features ...................................................................................................................................... 8  
Hardware Specifications ..................................................................................................................... 9  
Installation Experience ...................................................................................................................... 9  
Minimum Requirements ..................................................................................................................... 10  
Target Audience ............................................................................................................................... 10  
Global Availability ............................................................................................................................ 10  
Contacting Trend Micro ..................................................................................................................... 10  
  - United States ............................................................................................................................... 10  
  - Japan ........................................................................................................................................... 10  
  - Australia and New Zealand .......................................................................................................... 11  
  - Singapore ................................................................................................................................... 11  
Free Phone, Email and Chat support ............................................................................................... 11  
Premium Support Services ............................................................................................................... 11  

**Section 2: The Home Network Security Application** ................................................................. 12  
Setup and Connection .......................................................................................................................... 12  
Dashboard ......................................................................................................................................... 18  
  - Check Devices ............................................................................................................................. 18  
  - Using the Dashboard .................................................................................................................... 21  
Timeline ........................................................................................................................................... 25  
Devices ............................................................................................................................................. 26  
Family ............................................................................................................................................... 27  
  - Add a Family Member and the Devices They Control ................................................................. 27  
  - Filtering ....................................................................................................................................... 29  
  - Inappropriate Apps ....................................................................................................................... 33  
  - Time Limits ................................................................................................................................. 34  
  - Connection Alert ......................................................................................................................... 37  
Network ............................................................................................................................................ 38  
Voice Control ..................................................................................................................................... 39
Section 3: Core Technologies ................................................................. 53
    Deep Packet Inspection (DPI) / Intrusion Prevention System (IPS) ............... 53
    Network Attacks .................................................................................. 54
    Web Threats ......................................................................................... 54
    Device and Application Management ....................................................... 55
    Automatic Device Recognition .............................................................. 55
    Automatic Vulnerability Scan ................................................................. 55
    Web Threat Protection (SPN) ................................................................ 55
    Network Attach Options ........................................................................ 56
About Trend Micro .................................................................................... 57
Executive Summary

Figure 1. Trend Micro Home Network Security Station

Trend Micro Home Network Security (HNS)—a combination network hardware and software solution—provides advanced protection against cyber-attacks for every internet-connected device in your home—including desktop and mobile devices, game consoles, smart TVs, and smart appliances.

Heralding a new era of security for connected consumer homes, Trend Micro Home Network Security uses advanced deep packet inspection technology to provide the security-aware family with an extra layer of protection and visibility for the home network and connected devices—and no endpoint security software installation is required. HNS’s enterprise-grade Intrusion Prevention (IPS) technology and Cloud Intelligence protects your entire network against hackers, identify theft, financial loss and privacy invasion.

An easy-to-use Home Network Security Smartphone App (HNS App) for Android and iOS mobile devices lets the “home technology manager” make changes on the go and stay aware of important security events in the home network with timely and insightful notifications.
Figure 2. Protecting Your Smart Home. Trend Micro Home Network Security attaches to your gateway or router to detect and block network attacks, intrusions, and Web threats for all the networked devices in your smart home—and includes easy-to-use parental controls to protect your children.

Trend Micro Home Network Security Highlights

Trend Micro Home Network Security (HNS) provides an easy-to-use security solution to protect all the devices on your network.

- **Secure Home Network.** Advanced, enterprise-grade Intrusion Prevention technology senses and blocks network attacks before they get to your devices. HNS scans your devices for vulnerabilities, to help you make sure that hackers can’t get in to your network.

- **Plug-n-Protect.** Unlike other security solutions requiring experts just to install it, our solution is a breeze to set up. Simply plug the HNS Station into your wireless router and a wall socket, download the mobile app, pair the app and the HNS Station—and your home network is immediately protected.

- **Home Device Management.** Check your security status in real-time and manage access for all the connected devices in your home—including your smart speakers, security cameras, smart TVs, mobile phones, and even smart home devices like lights and door locks.

- **Parental Controls for Kids and Family.** Set time limits on game consoles. Block access during homework and family time. Prevent mature content from making it to the screens of the immature. Know what they’re doing online so you can teach them about using the Internet safely.

- **Anywhere, Anytime Visibility and Control.** Manage your network with our easy-to-use, real-time smartphone app. Customize the internet for family and guests at the touch of
a button. Grant or block access to new computers, phones, tablets, or smart home devices entering your network.

- **World-Class Protection.** Trend Micro Home Network Security taps into Trend Micro’s World-Class AI security system, enabled by the Smart Protection Network (SPN). Your home network and all the devices on it are protected from a wide range of threats, including network intrusions, malicious websites and files, default or weak passwords on your network devices, intranet or internet-based malicious behavior, system vulnerabilities, and privacy and network access violations.

- **New! Voice Control.** In HNS version 2.0 you can now use Amazon Alexa voice control to execute commands through your Echo smart speaker to perform specific functions on Trend Micro Home Network Security. [See Echo - Alexa Voice Commands](#) for a list of commands.

- **New! Advanced Vulnerability Detection.** In HNS version 2.0, a new Vulnerability Check has been added to the Device Scan which assesses connected devices for high-severity vulnerabilities that have been exploited in the wild. Once a vulnerability is detected, HNS provides users with guidance on how to resolve the vulnerability.

- **New! Early Access Program.** HNS users now have the opportunity to try the very latest in security and protection for their network and devices. Early Access features include:
  - **Router Access Protection.** HNS helps prevent hackers from gaining control of your router and making changes to important settings that can leave your network and devices vulnerable. With Router Access Protection enabled, all attempts to login to your router will be blocked unless approved.
  - **Ad Block.** HNS helps you protect your family’s privacy by blocking ads on all devices. It also brings the added benefit of faster load times for some sites.
  - **Cyberattack Shield.** HNS will deploy real-time emergency security policy to your network from the cloud in case of a global threat outbreak to prevent further spreading of threats like ransomware and botnets.
Section 1: Detailed Product Specifications

Key Features

Table 1. Trend Micro Home Network Security Key Features

<table>
<thead>
<tr>
<th>Category</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECURITY</td>
<td></td>
</tr>
<tr>
<td>Threat Blocking</td>
<td>Internet (WAN) Traffic*</td>
</tr>
<tr>
<td></td>
<td>Local (LAN) Traffic*</td>
</tr>
<tr>
<td>Web Threat Protection</td>
<td>Web Reputation Filtering</td>
</tr>
<tr>
<td></td>
<td>Cloud File Scan</td>
</tr>
<tr>
<td>ACCESS CONTROL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>New Device Approval</td>
</tr>
<tr>
<td></td>
<td>Remote Access Protection</td>
</tr>
<tr>
<td>DEVICE SCAN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Password Check</td>
</tr>
<tr>
<td></td>
<td>Vulnerability Check</td>
</tr>
<tr>
<td>PARENTAL CONTROLS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>WEB ACCESS CONTROL AND MONITORING</td>
<td>Daily Time Quota</td>
</tr>
<tr>
<td></td>
<td>Customizable Schedule</td>
</tr>
<tr>
<td></td>
<td>Pause Internet Access by Profile</td>
</tr>
<tr>
<td></td>
<td>Online Connectivity Monitoring</td>
</tr>
<tr>
<td>WEBSITE &amp; CONTENT FILTERING</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Website Filtering</td>
</tr>
<tr>
<td></td>
<td>Google Safe Search</td>
</tr>
<tr>
<td></td>
<td>YouTube Restricted Mode</td>
</tr>
<tr>
<td>APP CONTROLS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>YouTube Pause and Time Limits</td>
</tr>
<tr>
<td></td>
<td>App Detection</td>
</tr>
<tr>
<td>MANAGEMENT</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>DEVICE MANAGEMENT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Profile-based Management</td>
</tr>
<tr>
<td></td>
<td>Device Management</td>
</tr>
<tr>
<td></td>
<td>Device Detection</td>
</tr>
<tr>
<td></td>
<td>Device Approval</td>
</tr>
<tr>
<td></td>
<td>Device Blocking</td>
</tr>
<tr>
<td>VISIBILITY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Notifications</td>
</tr>
<tr>
<td></td>
<td>Dashboard</td>
</tr>
<tr>
<td></td>
<td>Timeline</td>
</tr>
<tr>
<td></td>
<td>Network Usage</td>
</tr>
<tr>
<td>USER INTERFACE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Smartphone / Tablet</td>
</tr>
<tr>
<td></td>
<td>Voice Control: Alexa</td>
</tr>
</tbody>
</table>

*WAN = Wide Area Network (Internet) | LAN = Local Area Network (Home Network)
Hardware Specifications

Table 2. Hardware Specifications

<table>
<thead>
<tr>
<th>Trend Micro Home Network Security Station</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions</td>
<td></td>
</tr>
<tr>
<td>Length: 136.27 mm</td>
<td></td>
</tr>
<tr>
<td>Width: 110.99 mm</td>
<td></td>
</tr>
<tr>
<td>Height: 31.20 mm</td>
<td></td>
</tr>
<tr>
<td>Color</td>
<td>Black</td>
</tr>
<tr>
<td>Weight</td>
<td>0.5 lb. (226 g)</td>
</tr>
<tr>
<td>CPU</td>
<td>Dual Core 1.3 GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>512 MB DDR3</td>
</tr>
<tr>
<td>Flash Memory</td>
<td>4 GB eMMC</td>
</tr>
<tr>
<td>Ports</td>
<td>1 Gbps Ethernet</td>
</tr>
<tr>
<td>Power Adaptor</td>
<td>AC Input: 90°-260 VAC</td>
</tr>
<tr>
<td></td>
<td>47°-63 Hz</td>
</tr>
<tr>
<td></td>
<td>DC Output: 12V/1A</td>
</tr>
<tr>
<td></td>
<td>Energy Star Version 2.0 Level VI efficiency requirements</td>
</tr>
</tbody>
</table>

Installation Experience

Even the most advanced security in the world means nothing if normal people can’t install it. Home Network Security’s set up is simple, fast and, in most cases, requires no network configuration on the user’s part. With most routers, the installation flow is as follows:

1. Plug the HNS Station into a free LAN port on your router and plug in the power.
2. Download and install the HNS app on your Android or iOS smartphone.
3. Pair the HNS Station and the HNS app on your smartphone to activate the service.

Figure 3. HNS Setup Flow
Minimum Requirements
The minimum requirements for using Trend Micro Home Network Security are:

- A working internet connection.
- A compatible router with a free LAN port. To ensure the optimal experience with Home Network Security make sure you are using a compatible router. Click here for a List of Compatible Routers.
- A smartphone or tablet: Android 5.0+ or iOS 11.0+.

Target Audience
The primary users of Trend Micro Home Network Security are the “house geek” who’s responsible for setting up the network and monitoring the smart devices in the home, while keeping them—and the family members who use them—safe from hackers and malware; and protective parents, who want to make sure their kids stay safe from threats and protected from unwanted content on the Internet.

Global Availability
Available now (2019) in the United States, Japan, Australia, New Zealand and Singapore.

Contacting Trend Micro

United States
Trend Micro Incorporated
225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900
Toll-free: (888) 762-8763
www.trendmicro.com

Japan
Shinjuku MAYNDS Tower
2-1-1 Yoyogi, Shibuya-ku
Tokyo, Japan ZIP 151-0053
Phone: +81.3.5334.3618
www.trendmicro.co.jp
Australia and New Zealand
Level 15, 1 Pacific Highway
North Sydney, NSW 2060
Australia
Toll-free: 1-800-642-421
www.trendmicro.com.au

Singapore
6 Temasek Boulevard #16-01 to 05 Suntec Tower Four
Singapore 038986
Phone: +65 6379 2060
www.trendmicro.com.sg

Free Phone, Email and Chat support
Trend Micro offers free phone, email, and chat support. For more info, go to [Trend Micro Home and Home Office Support](https://www.trendmicro.com) and more specifically to the [Trend Micro Home Network Security](https://www.trendmicro.com) support page.

You can also go to the [Trend Micro Home Users Community](https://www.trendmicro.com) to get your questions answered and problems solved.

Free ransomware-specific tech support is provided for all users, whether you are a customer or not, by calling 1-877-558-7363 between 5:00 a.m. to 9:00 p.m. PST, Monday through Friday.

Premium Support Services
Trend Micro provides users with [Premium Support Services](https://www.trendmicro.com) for a wide variety of technical issues including installation, virus and spyware removal, PC Tune-ups, etc. These services are offered as a bundle with a purchase of Trend Micro Security or as stand-alone and ad-hoc services.
Section 2: The Home Network Security Application

The Home Network Security Smartphone Application (HNS App) provides setup, monitoring and control of your Home Network Security Station (HNS Station) and all of the devices it protects on your network.

(In the following screens, the HNS App version shown is v2.0.1516, taken from an Android device. The screens for the iOS version are identical.)

Setup and Connection

To set up the Station:

1. Plug the power adaptor and the Ethernet/LAN cable into the Station.
2. Connect the Station to one of your wireless router’s Ethernet/LAN ports and plug the power adapter into a power outlet.
3. When the light is green, the Station is ready to set up.
4. If the light remains red for more than 1 minute, consult the Light Status table shown here.
5. If the Station doesn’t achieve a steady green, you may need to reset the device by pushing a paperclip end into the Reset button for 5 seconds.

<table>
<thead>
<tr>
<th>Light Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steady Green</td>
<td>Normal</td>
</tr>
<tr>
<td>Blinking Green</td>
<td>Ready to setup</td>
</tr>
<tr>
<td>Steady Red</td>
<td>No internet connection or subscription has expired</td>
</tr>
<tr>
<td>Blinking Red</td>
<td>The Station is starting or updating firmware. Please wait until the light is green.</td>
</tr>
<tr>
<td>Blinking Red and Green</td>
<td>System error</td>
</tr>
</tbody>
</table>

Figure 4. Back: Home Network Security – Power Adaptor, Reset Button, Router Ethernet Port Connection

Figure 5. Front: Station Ready

Figure 6. Light Status

Commented [MM12]: True?
6. When the light on the Station is blinking green, connect your phone to the same Wi-Fi network as the Station.

Figure 7. Connect to Same Wi-Fi Network

7. Launch Google Play (or the Apple App Store) and search for Trend Micro Home Network Security.

8. When it appears, tap Home Network Security, then Install.

Figure 8. Google Play > Home Network Security

Figure 9. Home Network Security Install

9. An app manifest appears, indicating what Home Network Security needs access to.

10. Review the access permissions you’ll grant to the app and if you agree, tap Accept.

11. Home Network Security downloads and installs. When the installation is complete, tap Open.

Figure 10. Home Network Security App Manifest

Figure 11. Home Network Security > Open
12. The Privacy and Personal Data Collection Disclosure appears.

13. If you agree to the terms, tap Accept and Continue. The Welcome screen appears.

14. Here you can read the Trend Micro License Agreement by tapping the link.

15. If you agree to the terms of the License Agreement, tap Accept and Continue.

16. When the screen to Connect to the Station appears, enter the 16-character Pairing Code (the code is case-sensitive) in the field provided and tap Next.

17. The Pairing Code will pair your HNS App to the HNS Station and activate the station.

Commented [MM13]: MP: My current pairing code doesn’t work. I’ve sent you an email about this.
18. When the connection is complete, a screen appears saying Connection Successful.

19. You’re then automatically taken to a screen to Sign In to your Trend Micro Account.

20. Enter the email address and password you used to purchase Home Network Security and activate your Trend Micro Account and tap Sign In.

21. Home Network Security then provides you with a series of demo screens informing you how you can use your Network security solution: Keep Track Using the Timeline.

22. Tap Next. You can See Who is Connected Using Devices.

23. Tap Next.
24. You can decide what your kids can see online and when they can use the Internet, to provide Safe Internet for Your Family.

25. Tap **Next**. You should Use Home Network Security with Your Anti-Virus Software; for example, with [Trend Micro Security](https://www.trendmicro.com) and [Trend Micro Mobile Security](https://www.trendmicro.com), for starters.

26. Tap **Next**.

27. Home Network Security automatically does a network check to see what devices are on your network.

28. When it’s completed the scan, a popup will appear to view the devices found on your network.

29. Tap the **View Devices** button to view your network devices.
30. Home Network Security provides you with a list of All Devices on the network.

31. View the Dashboard items by scrolling down the Dashboard screen.

32. Tap Family Members: Assign Now to begin to creating family members and assigning devices to them. (See the Family section below to learn how to do this.)

33. Congratulations! You’re all set up! You may now begin using Trend Micro Home Network Security to monitor and manage the safety and security of all the connected devices on your home network, including PCs, Macs, smartphones and tablets, TVs, security cameras, thermostats, and smart speakers, etc.
Dashboard

The HNS App’s Dashboard provides a quick overview of all the monitoring and security functions of Home Network Security, with easy-to-use screens showing the security status of all the connected devices on your network.

Check Devices

To check devices and actions required:

1. Tap the Home Network Security (HNS) icon on your home screen of your mobile device to open the HNS App Console. The Console opens and displays the Dashboard.

2. You can access any screen in the Console by tapping the Command Menu icon in the upper left-hand corner. The Command Menu displays, with menu items for all the main functions of the HNS App.

Figure 28. Dashboard | Command Menu

Figure 29. Command Menu > Dashboard Menu Item
3. If there are any past Action Required items, they'll display in the Dashboard indicator at the top; just tap to review them.

4. To find all the connected devices on your network and to check their security, tap Check Devices.

5. HNS conducts a network scan to determine what devices are connected to your network and to check their security status, providing a Progress Indicator and a popup showing the progress of the scan.

6. While the scan is being conducted, you can tap the Back-Arrow on your device to go back to the Dashboard.

7. The Check Devices button now shows Checking Progress.

8. When the scan is done it returns the result. In this example, 1 Vulnerability Found.

9. Tap View Now to view the issue it has found.
10. In this example, the Action Required screen indicates that a network printer has been discovered with an SSL-Poodle Vulnerability.

11. Tap the panel to obtain the Issue Details. Read the Potential Risk description to understand the issue.

12. Tap Recommended Actions to see what you can do to resolve the issue. (You can also tap Skip for Now to skip the remediation process.)

13. The HNS App loads your mobile browser and takes you to the Trend Micro eSupport site, which provides more details on the issue and recommended actions.

14. Scroll through the page to learn more about the possible risks, what you can do to prevent the problem from happening in the future, and places to go for more answers to any questions you may have about the issue.
Using the Dashboard

To review Dashboard items:


2. Tap the link Show More/Show Less to show more or less detail, respectively.

3. Tap individual items, e.g., Vulnerability Found, Network Attacks, Web Threats Blocked, etc., to reveal information on the various threats by device.

4. Tap individual panels to show additional details about particular attacks or threats.
5. Do the same for Remote Connections, Total Devices Protected.

6. Again, tap individual panels to show details about the particular security issue: e.g. the Remote Access application blocked.

7. Tap the Parental Controls panel to view Inappropriate Websites Blocked or Visited.

8. Tap the panels for the individual instances to get more details on the violation.

9. In the Family Members panel, tap an individual family member to access the Report, Settings, and Device(s) controlled by the member.
10. The family member’s Report informs you about their Internet Use Today, including the Total number of hours and minutes used, and the total amount of time they spent watching YouTube.

11. Tap the Pause buttons to Pause Internet or Pause YouTube for that family member. Tap it again to Resume the usage.

12. Tap the Settings tab to set up Parental Controls for that person. Here you can set up Filtering, Inappropriate App(s) Used, Time Limits, and Connection Alerts. (See the Family section for setup details.)

13. Tap the Device tab to see a list of the devices controlled by the family member, then tap any individual device icon for more details about it.

14. In the device’s Settings tab, toggle Connect to the Network On or Off, to control the device’s access to the network.

15. Tap the specific device information, e.g., Owner, Name, Type, etc., to assign new ownership or to view or edit the item, using the relevant menu or editor.
16. Tap the **Report** tab to obtain a Protection Report for the various categories of protection; then tap individual panels for more details on that section of the report.

![Figure 50. Device Report](image1)

![Figure 51. Remote Access Risk Blocked](image2)

17. The **Report** and **Settings** tabs for devices are also available by tapping a device icon in the Top Attacked Devices section of the Dashboard.

18. Back in the bottom of the main Dashboard screen, tap **Network Usage** to obtain Download and Upload network consumption for the Last 7 or 30 Days, with a graph showing overall consumption and a list of Download/Upload consumption by device.

![Figure 52. Network Usage](image3)

![Figure 53. Network Usage > Last 30 Days](image4)
Timeline

The **Timeline** provides a handy list by date of all issues discovered by Home Network Security, letting you monitor or take action to address them.

To use the Timeline:

1. Tap **Timeline** in the Command Menu. The Timeline displays.
2. Review all items in the Timeline by tap-holding and scrolling down the screen.
3. Tap individual items to display the Issue Details.
4. As previously noted, tap **Recommend Actions**, if available, to obtain instructions for what you can do to address the problem.
Devices

The Devices function lets you view All Devices or Online Devices assigned or unassigned to family members.

To use Devices:

1. Tap Devices in the Command Menu. The Devices screen appears.
2. Use the drop-down menu at the top to filter the Devices list by All Devices or Online Devices.
3. Tap the icon for an individual device to display the Settings screen for the device.
4. Tap Owner to change the owner to another family member, guest, or to move the device back to the unassigned list by tapping Move to Unassigned.
5. Edit fields or selection menus allow you to edit/change items in the other settings.
6. As previously indicated, the Report tab provides details on security issues pertaining to the device.
Family
You can add new family members and the devices they control. You can also set up Parental Controls for any family member and their devices, using the Filtering function to block Inappropriate Websites and Content. You can also block Inappropriate Apps, set Time Limits for internet use, and get a Connection Alert in your device’s pull-down Notification menu whenever the family member’s devices try to connect within the preset monitoring period.

Add a Family Member and the Devices They Control
To add a family member:

1. Tap Family in the Command Menu. The Family member list appears.
2. Scroll down the Family member list and tap the Plus (+) button to Add Someone.

Figure 62. Family Menu Item
Figure 63. Family Member List > Add Someone (+)
3. In the **Name** field of the **Name This Person** screen, type a name, then tap **Next**.

4. **Choose a Picture** to help you identify the family member in your **Family Member** list, then tap **Next**.

5. **Assign Devices** to the person by tapping the device(s) in the **Unassigned** panel. The devices you select will move into the ownership panel for that person.

6. Tap **Done**. You’re then presented with the **Settings** screen for that person (see below), where you can apply **Parental Controls** as you see fit.

(See the following **Filtering** section to begin setting up controls for the family member.)
Filtering

To set up Filtering:

1. To begin setting up Parental Controls for a family member, tap their icon from the Family Members List, or following on the instruction above, when you create a new member you’re presented with the Settings screen, where you can immediately begin setting up Filtering.

2. Tap Set Up Now for Filtering to block inappropriate websites and content for this family member. The Filtering screen appears.
3. Toggle on Get Notifications for this family member when selected websites are visited.

4. Toggle on Block to block selected websites for this family member.

5. Tap the Age Level for this child, or tap Custom to manually select categories and subcategories to block.

6. You may begin with an Age Level filter and customize it.

7. Add items in the Adult or Sexual category by tapping the checkbox(es).

8. Check items in the Communication or Media list.

9. Do the same for Shopping and Entertainment.
10. Back in the **Filtering** screen, tap **Set Exceptions** to set them.

11. Tap **Allowed List** or **Denied List** to add exceptions to that list.

12. Tap **Add a new website** to add the exception to the list.

13. Type in the URL for the website you wish to add, then tap **Done**.
14. The website is added to the list.

15. Tap the website in the list to test it. The Denied Website screen appears.

16. Tap **Open This Website** to test it.

17. HNS loads your browser and blocks you from going to the website, providing an **Off Limits** notice. This is the notice the family member will see when they attempt to go to this website.

18. Back in the Denied Website screen, tap **Remove This Website** to remove it from the list.

19. Toggle on **Google SafeSearch** to filter explicit search results in the family member’s mobile browser and **YouTube Restricted Mode** to filter out mature content on YouTube.
Inappropriate Apps

To set up Inappropriate App Used:

1. To set up Inappropriate App Used, tap Set Up Now. The Inappropriate App Used screen appears.

2. Tap Get Notifications to toggle the feature On.

3. Tap the checkboxes for App Categories you wish to receive notifications for.
Time Limits
To set up Time Limits:

1. To set up Time Limits tap Set Up Now. The Time Limits screen appears.
2. Tap Add First Rule to add it.
3. Select the Days for this rule; e.g., Mon-Fri.
4. Set the Internet Time Limit and Time on YouTube by scrolling back and forth to see the limits available, then tap the limits you want to set them.
5. Toggle on Get Notifications.
6. Set the time period when the family member can use the Internet by tapping the From field, then move the Time wheelbar to the Beginning time.

7. When the wheelbar sets the time, tap AM or PM to set it, then OK.

8. Do the same operations for the Ending time and tap OK.

9. Toggle on Get Notifications and Block Internet Access, for when the Internet is used outside of the time period.

10. Tap Add another time period if you wish and repeat the processes outlined above.

11. Tap Next to complete the rule setup.
12. When you have finished setting the rule(s), the **Rule Complete** screen shows a summary of the rule you set, providing a clock to show the **Allowed Time**, the **Days** for which the rule is set, the **Hours** of Internet allowed, including any time allowed for **YouTube** viewing, and the **Times** allowed.

13. Tap **Done** to finalize the rule. The **Time Limits** screen shows you the rule for the family member. Toggle the rule **Off** if you wish, or **Add new rule** to set a new rule.
Connection Alert

To set up Connection Alert:

1. Tap Set Up Now to set up Connection Alert.

2. Tap the Get Notifications toggle to On, then tap the checkboxes of individual devices Off in the Select Device panel to remove the device for the monitoring period (i.e., when they connect to the internet between 12 and 10pm.)

3. Tap the back arrow to return to the main screen for the family member.

4. All Parental Controls for the family member have now been set to On.

5. If you wish to remove the family member from the family group, tap Remove This Person. Once a family member has been removed, their devices will return to the Unassigned group.

Figure 95. Set Up Connection Alert

Figure 96. Get Notifications for Devices Connecting to Internet

Figure 97. Parental Controls Set for Family Member
Network

The **Network** control allows you to view the total amount of data you’ve downloaded and uploaded over your network for the Last 7 or 30 Days. It also provides individual upload and download amounts per device.

1. Tap **Network** in the **Command Menu** to display the **Network** screen.

2. View the graph by date for the total amount downloaded and uploaded over the network for the **Last 7 Days**, as well as the amounts downloaded and uploaded per device.

3. Tap **Last 30 Days** to view the graph and data for the past 30 days.
Voice Control

Voice Control lets you give voice commands through Alexa to the Amazon Echo smart speaker to conduct a scan and obtain security data from Home Network Security. To use this feature you need an Amazon Echo or Alexa-enabled device and a valid Amazon account.

To use Alexa Voice Control:

1. Tap Voice Control in the Command Menu. The Voice Control demo page appears.
2. Tap View on Amazon to enable Voice Control for your HNS Station via your Amazon Echo.

![Voice Control](image1.png)

![View on Amazon](image2.png)
3. The HNS App loads your browser and takes you to the Amazon login page to enable you to Sign In to your Amazon account to enable Voice Control.

4. Here we assume you’ve already created your Amazon account. Simply add your email address and password to the entry fields and tap Sign In.

5. In the Trend Micro Home Network Security enabling page, tap Enable to enable Voice Control.

6. You’re taken to the Home Network Security Trend Micro Account page to sign in with your Trend Micro Account to connect to Alexa.

7. Enter the email address and password you used to create your account and tap Sign In.
8. As you proceed through the Account Linking process, you’re notified as you go along.

9. Once completed, you’re informed that Trend Micro Home Network Security has been successfully linked in your Amazon Alexa skill page.

10. Tap Close to close the linking page.

11. You now have five Voice Control Commands ("intents") you may now use via Alexa to control your HNS Station.

12. The following launch request opens a skill without an intent:
   “Alexa, open Trend Micro.”
13. The following commands open a skill with an intent.

14. “Alexa, ask Trend Micro if my network is OK.”

15. “Alex, ask Trend Micro what Tom (or other name) did today.”

16. “Alexa, ask Trend Micro to pause the Internet for Tom (or other name).”

17. “Alexa, ask Trend Micro to turn off YouTube for Tom (or other name).”
18. “Alexa, tell Trend Micro to scan my network.”

19. At any time, if you wish to disable Voice Commands via Alexa, simply log into your Amazon account by tapping View on Amazon, log in, then tap Disable Skill.

20. Voice Commands will be disabled on your HNS Station.
Help

Home Network Security provides various kinds of Help, to facilitate the smooth operation of the HNS Station.

To obtain Help:

1. Tap Help in the Command Menu. The Help screen appears.
2. Here you’ll find a phone number to Contact Support.
3. You can also tap Request a call from Support; enter your phone number in the form provided.
4. If need be, scroll down the screen to reveal more items.
5. Tap the items in the Troubleshooting section, or the How Do I section to take you to individual Help pages.

Commented [MM14]: There is no US or NABU number here for Support

Commented [MM15R14]: Since I’m using a Beta version of HNS, I also don’t have these intermediate screens. Is this OK?
Settings

The Settings in the HNS App help you set up and configure Home Network Security to fit your needs.

To configure Settings:

1. Tap Settings in the Command Menu to open the Settings screen.
2. Tap Threat Blocking to configure the settings that block threats.
3. **Toggle On/Off Network Protection.**
When this protection is On, HNS helps prevent external attacks and malicious network behavior using its IPS protection.

4. To help prevent attacks between devices in your home network, tap **Internal Attack Blocking.**

5. A popup appears, indicating that some routers may not fully support this feature, you may have instability issues.

6. Tap **Web Threat Protection** on the Threat Blocking screen to open the settings.

7. **Toggle On/Off Dangerous Websites Blocked and Dangerous Files Blocked.**

8. Tap **Approved List** to add websites to the list.

9. Tap **Add a new website** to add a new website by entering the URL in the entry field provided.
10. Back in the main Settings page, tap Access Control to access the settings.

11. Tap Remote Access Protection to limit remote access connections to your devices.

12. Toggle Block Remote Access On/Off to control the function.

13. Tap Approved List to add an approved remote access program to the list.

14. Tap Add Program to add programs, or tap existing apps to remove them from the list.

15. Back in the main Settings screen, tap Device Scan to access the Device Scan settings.

16. Toggle Password Check and Vulnerability Check On/Off to control the settings.
17. Back in the main Settings screen, tap Notifications to access the settings for notifications.

**NOTE:** Notifications show up in the drop-down menu of your device.

18. Tap **Network Attacks Blocked** to choose the notifications options:

- No Notifications
- Only Notify Me for High Severity Attacks
- Notify Me for All Attacks

19. Toggle the various other options On/Off to Enable/Disable the respective setting.
20. Continuing in the Notifications screen, tap Remote Access Protection to access the various options:
   - No notifications
   - Notify me when remote access connections are blocked
   - Notify me for all remote access connections

21. Back in the main Settings screen, tap Early Access Program to access the settings.

22. Enable the Early Access features to be the first to try the latest protections and give feedback.

23. Toggle the Early Access Notification On/Off to Enable/Disable the notification.

24. Toggle Router Access Protection and Ad Block On to test and give feedback.


26. Tap Unmanaged Devices to add such devices or to remove them from the Managed Devices list.
27. Tap **Station Configuration** to change the **Mode** for your router, or to enable DHCP Mode. (See **Network Attach Options** in the following section).

28. Once you’ve made your change, tap **Test Status** to ensure the change has taken effect and the HNS Station is functioning well.

29. If it is, you’ll see a **Dangerous Page** alert showing the test website has been blocked.

30. In the main **Settings** screen, tap **Station Management** to access the settings.

31. If you wish to **End Station Management**, tap the setting.
32. A popup appears, asking if you really wish to End Station Management?

33. Tap Cancel to abort the process, or End to End Station Management.

34. To Reset the Station, tap the setting.

35. A popup appears, asking if you sure you wish to Reset the Station? All of your data will be deleted.

36. Tap Cancel to abort the process, or Reset to complete it.


39. Back in the main Settings page, toggle On/Off Help Improve This App, to share/not share anonymous data with Trend Micro.

40. Tap Give Feedback to send feedback to Trend Micro about Home Network Security.

41. During a troubleshooting session with a Trend Micro Support Technician, you may be asked to Send Troubleshooting Logs to help solve your problem. Simply tap this function when asked.
Section 3: Core Technologies

Trend Micro Home Network Security provides an array of technologies that enable the key functions of the solution. These include:

- A Deep Packet Inspection (DPI) engine / Intrusion Prevention System (IPS)
- Automatic Device Recognition
- Automatic Vulnerability Scan
- Web Threat Protection
- Network Attach Options

Deep Packet Inspection (DPI) / Intrusion Prevention System (IPS)

HNS’s Intrusion Prevention System (IPS) security technology covers a broad spectrum of threats and vulnerabilities that home networks face today. Behind HNS’s IPS is the Deep Packet Inspection (DPI) engine, an advanced technology for analyzing and managing network traffic.

DPI goes beyond packet filtering, which only analyzes packet headers, by inspecting the data and payload of the traffic. This scan returns multiple results for security and management applications in a performant, single-pass process. This approach allows HNS to protect you and your devices against sophisticated network intrusion and device compromise attempts while minimizing impact on network throughput.

The threat coverage of IPS far exceeds the protection provided by DNS-based security implementations in a number of important areas, including device compromise through inbound attacks that use techniques like brute force logins and exploit system vulnerabilities.

Figure 147. HNS Single-Pass DPI Scan Engine
Network Attacks
Where HNS’s IPS protection really shines is detecting and blocking network attacks. Because it scans traffic coming in and going out of a network, HNS’s IPS is able to protect consumer home networks against inbound device compromise attempts, remote device control (botnets) and even cryptocurrency mining. Recent and well-known examples of these types of threats include WannaCry, Heartbleed and Shellshock. DNS-based solutions aren’t able to see or analyze these attack attempts, let alone block them from reaching their targeted victims.

Web Threats
By forwarding URL requests to Trend Micro’s Smart Protection Network (SPN), HNS’s IPS is able to provide granular and accurate web-threat protection to consumers. DNS-based solutions are limited when it comes to URL filtering because the precision of their reputation systems only cover the domain of a requested URL. In addition, any requests which directly use an IP address are not covered by a DNS-based solution. Trend Micro’s own data shows that two-thirds of all web threats are matched at the directory or URL level, not the domain level, indicating that a majority of web threats could be missed by DNS-based solutions.

Trend Micro’s SPN also dynamically scans potentially executable files, including .EXE and .PDF files, in the cloud and in real-time to ensure that those files are not malware.

Table 5. Threat coverage of DPI-based IPS vs DNS-based security

<table>
<thead>
<tr>
<th>Threat Category</th>
<th>HNS (DPI-based IPS)</th>
<th>DNS-based Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Threats</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Reputation</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>URL Reputation</td>
<td>Yes</td>
<td>Partial (domain-level only)</td>
</tr>
<tr>
<td>Dynamic Cloud-based File Scan</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Inbound Device Compromise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brute Force Login</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Default Credential Exploitation</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Vulnerability Exploitation</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Remote Device Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Botnet Participation via DoS/DDoS</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Others</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cryptocurrency Mining</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Device and Application Management

Additional benefits of DPI include the identification and management of devices and applications. Metadata picked up during traffic inspection allows Trend Micro to show consumers the devices that are connected to their network as well as the applications that are in use. Beyond visibility, DPI allows for the management of those devices and applications, including allowing or blocking devices and applications and setting time limits.

Automatic Device Recognition

Automatic Device Recognition takes the output of an active network scan, which analyzes the response metadata to assess a device’s brand, model and category. Metadata from scanned network traffic offers additional input used in recognition.

In cases where the recognition is incomplete or inaccurate, users can modify the recognition result generated by HNS. That learning is fed back into the system to improve recognition going forward.

Automatic Vulnerability Scan

HNS’s Automatic Vulnerability Scan probes for default/weak password settings on devices that have administrative consoles like routers, IP cameras and network attached storage (NAS) units.

After version 2.0 has been released (Fall 2019), high severity vulnerabilities like Heartbleed and Poodle will be tested for in connected devices. If found, users will be provided with a notice giving advice on how to mitigate the vulnerability (like updating their device’s firmware).

Web Threat Protection (SPN)

Trend Micro maintains one of the world’s largest web reputation databases—a key component of the Trend Micro Smart Protection Network (SPN), which also includes world-class file and email reputation databases, as well as other advanced technologies including Trend Micro™ XGen machine learning, the artificial intelligence powering Trend Micro Home Network Security.

With its Web Threat Protection (WTP) technology, websites are scored on age, location changes, and suspicious behavior. Through a two-tier system, Trend Micro examines both single and multi-component testing of web sites, sandboxing and testing of new components on existing sites, and monitoring of cyber-criminal activity. Real-time page analysis, using script analyzers and browser exploit prevention technology, identifies new malicious URLs at the time of access. The result is industry-leading blocking of both existing and evolving web threats to Trend Micro’s customers.

In short, Trend Micro Home Network Security’s Web Threat Protection (WTP) feature taps into the SPN’s web reputation database as soon as it’s installed, ensuring the safety of your home users whenever they access the web on any device that’s part of your network. If a user clicks a bad link in a browser, an email or instant message, or on a social networking site, they’re instantly notified and blocked from going to the malicious website—and the

Commented [MM18]: Added more descriptive words to better define what exactly is going on with these technologies, i.e., “automatic” “recognition” “device-policy assignment” etc.

Commented [M(19R18]: great, I have no issue

Commented [MM20]: Check for the three types of blocking. Are all types supported?

Commented [M(21R20]: Yes, unless the requests are encrypted
home network administrator is notified of the blocking action, by user and device, as part of HNS’s normal reporting mechanism.

## Network Attach Options

HNS acts as the gateway when attached to the network router in the following ways:

- **Automatically.** Setup occurs without user configuration, by utilizing ARP Spoofing. This technique is important for helping get even the least tech-savvy customer up and running and their network and devices secured. No decision-making or networking knowledge is required on the part of the user when using this mode.

![Routing Under Normal Conditions](image1)

**Figure 148. HNS ARP Spoofing for MITM Security**

- **Mode 1, Mode 2, Mode 3.** Mode 1 is the default setting. Mode 2 or Mode 3, which are also ARP Spoofing modes, may be triggered automatically or can be used manually (just tap the option) if you are experiencing network issues or are having problems connecting to the Internet. If you change the mode, run a Test Status check 5 minutes after changing the settings.

- **DHCP Mode.** Using DHCP Mode you can configure Home Network Security as a DHCP Server. Enabling DHCP Mode requires you to first disable the router’s DHCP server. With a small number of routers, this configuration is required so HNS can secure the network and devices. Also, some more technical customers who are willing and able may feel more comfortable with this setup and make the changes themselves.

HNS will attempt to determine the correct method during the setup process based on the router it is connected to. Most routers support the automatic method, though a very small number do require manual setup. An even smaller number are not compatible with HNS.

To ensure the optimal experience with Home Network Security, make sure you are using a compatible router. Click here for a List of Compatible Routers.
About Trend Micro

Trend Micro Incorporated, a global leader in cyber security solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world’s most advanced global threat intelligence, Trend Micro enables users to enjoy their digital lives safely.

For more information, visit Trend Micro Security for Home or Home Network Security.