Deep Discovery Inspector is a third-generation threat management solution that delivers advanced persistent threat (APT) and targeted attack visibility, insight, and control. Deep Discovery Inspector provides IT administrators with critical security information, advanced persistent threat (APT) and targeted attack visibility, insight, and control.

Deep Discovery Inspector is a third-generation threat management solution that delivers

## Verifying the Deep Discovery Inspector Carton

Verify that the Deep Discovery Inspector carton contains the following items:

1. Rack rails
2. Document and DVD
3. Power cords
4. Deep Discovery Inspector appliance

## Examining the Deep Discovery Inspector Appliance

1. Power-on button/indicator (10)
2. Front ID button/indicator (11)
3. LCD menu button (12)
4. LCD panel (13)
5. USB keyboard (14)
6. USB mouse (15)
7. Hard drives (4)
8. USB 2.0 connector (16)
9. Optical drive (17)
10. Data port 1 (1 Gbps) (18)
11. RS-232 serial connector (19)
12. Management port (20)
13. ORACLE port (21)
14. Data port 1 (1 Gbps) (22)
15. Data port 2 (1 Gbps) (23)
16. Data port 3 (1 Gbps) (24)
17. Data port 4 (1 Gbps) (25)
18. Rear video connector (26)

## Setting Up the Hardware

1. Mount the Deep Discovery Inspector appliance in a standard 19-inch 4-post rack, or on a freestanding object, such as a sturdy desk.
2. Connect the appliance to a power source.
3. Connect the monitor to the VGA port at the back of the appliance.
4. Connect the keyboard and mouse to the USB ports at the back of the appliance.
5. Connect the management port to your network.
6. Power on the appliance.

## Performing Initial Configuration: Management Console

1. Using a supported web browser, open the management console at: `http://<Deep Discovery Inspector IP Address>`
2. On the login screen, type the following default credentials:
   - **User name:** admin
   - **Password:** admin
3. Click Log On.
4. Type a new password, and then retype it to confirm.
5. Navigate to **Device Administration > License**
6. Click **Admin**.
7. Set the Internet Security level to Medium. Enable ActiveX Binary and Script.
8. Use the IP address that you specified during the initial configuration.
9. To configure post-deployment settings, follow the steps in the Setup Guide. For details on how to set up your threat protection, see the Get Started chapter in the Administrator’s Guide.
10. Connect one or more cables from the traffic source to any port of the appliance except the management port.

## Recommended Network Environment

Deep Discovery Inspector is deployed offline. This means that Deep Discovery Inspector does not interrupt network traffic. A switch monitors both internal and external traffic and passes the information to Deep Discovery Inspector. Deep Discovery Inspector uses this information to monitor known and potential threats.

You can connect switches with a mirror port to any of the ports except the management port. Deep Discovery Inspector uses these ports as listening ports and will not interrupt traffic handled by the switches.

Trend Micro recommends using a custom network for sample analysis. Custom networks ideally are connected to the Internet but may be configured with their own network settings. The appliance provides the option to configure proxies for custom networks, as well as providing support for proxy authentication.

The networks must be independent of each other so that malicious samples in the custom network do not affect hosts in the management network.

To plan your network deployment environment, see the Deployment section in the Installation and Deployment Guide.

## Deployment Checklist

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Code</td>
<td>Obtain from Trend Micro</td>
</tr>
<tr>
<td>Monitor and VGA cable</td>
<td>Connects to the VGA port of the appliance</td>
</tr>
<tr>
<td>USB keyboard</td>
<td>Connects to the USB port of the appliance</td>
</tr>
<tr>
<td>USB mouse</td>
<td>Connects to the USB port of the appliance</td>
</tr>
<tr>
<td>Ethernet cables</td>
<td>One cable connects the management port of the appliance to the management network. (Optional) One cable connects a custom network that is reserved for an internal Virtual Analyzer with any port of the appliance except the management port.</td>
</tr>
<tr>
<td>Internet-enabled computer</td>
<td>A computer with the following software installed: Google™ Chrome™, Microsoft™ Internet Explorer™ 11.0, and Mozilla Firefox™</td>
</tr>
<tr>
<td>IP addresses</td>
<td>One static IP address is the management network. (Optional) One additional IP address for an internal Virtual Analyzer if connected to a custom network with Internet connectivity</td>
</tr>
</tbody>
</table>

## Contact Information

- **Website:** http://www.trendmicro.com
- **List of worldwide offices and phone numbers:** http://www.trendmicro.com/us/about-us/contact/index.html

© 2017 Trend Micro Incorporated. All rights reserved. Trend Micro, the t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.