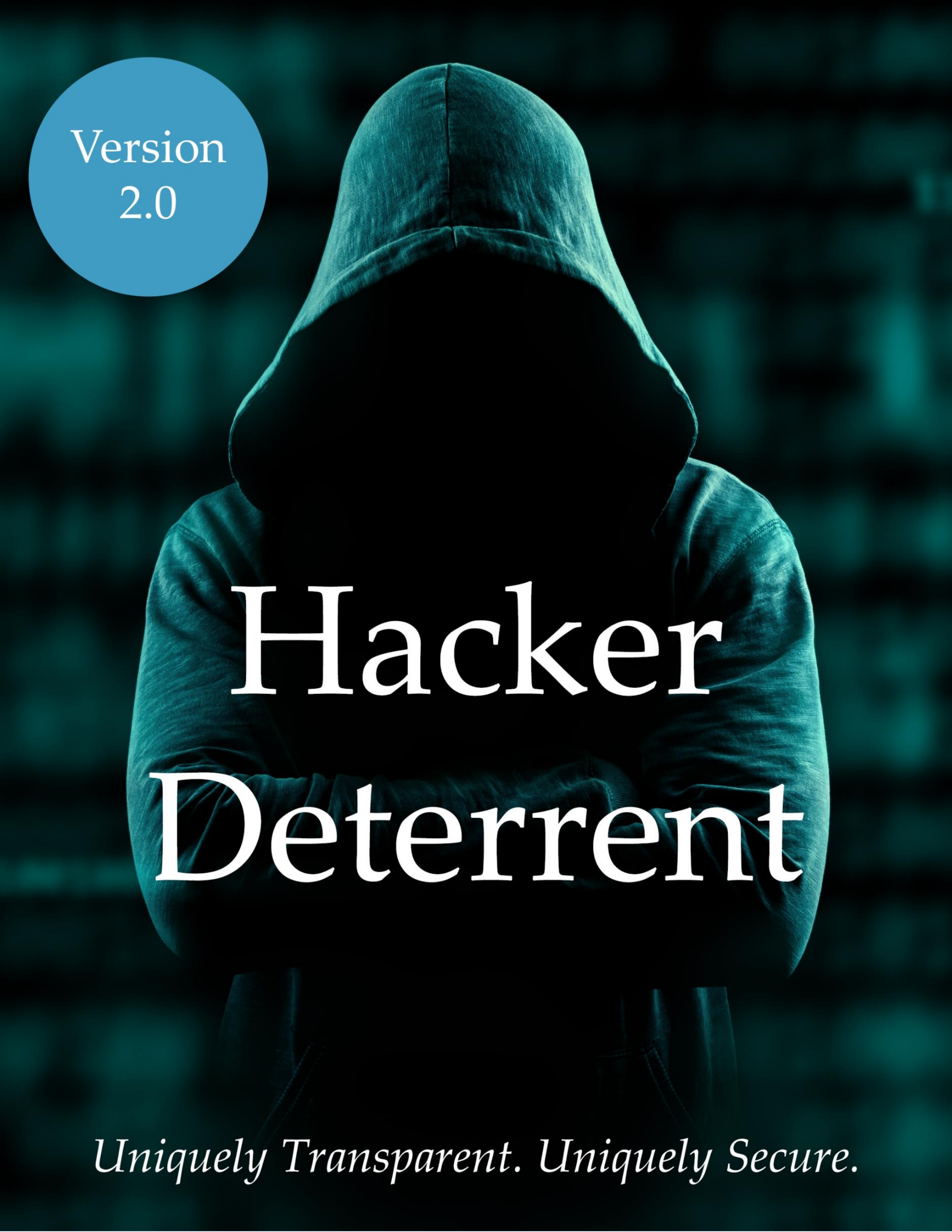


Version 2.0

Hacker Deterrent

Uniquely Transparent. Uniquely Secure.

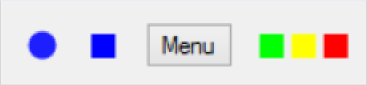
Important

You must keep Hacker Deterrent open at all times. For your security, Hacker Deterrent blocks all new sites when closed. Therefore, you must keep it open at all times. Click the blue square to reduce the window size.

Easiest Way to Use Hacker Deterrent

If you want maximum security and ease-of-use, we recommend that you combine Hacker Deterrent with Malwarebytes Anti-Exploit. Hacker Deterrent automatically blocks all applications from accessing the internet except for browsers. Meanwhile, Malwarebytes Anti-Exploit is especially effective for shielding one type of application: browsers. Working together, this powerful one-two punch delivers automatic security and convenience.

When using Malwarebytes Anti-Exploit, you will no longer need to manage the green or yellow browser traffic in Hacker Deterrent. Therefore, to use Hacker Deterrent with Malwarebytes Anti-Exploit:



- **Click the Green Square:** This filters all green allowed traffic. You no longer need to manage this traffic when Malwarebytes is running.
- **Click the Yellow Square:** This filters all yellow allowed traffic. You no longer need to manage this traffic when Malwarebytes is running.
- **Run Malewarebytes Anti-Exploit:** For download link and info see: https://blog.terraprivacy.com/2016/11/21/maximum-security-a-one-two-punch/

By removing the green and yellow traffic from the display, you reduce the number of entries by 90% or more — making it easy to control the little remaining traffic.

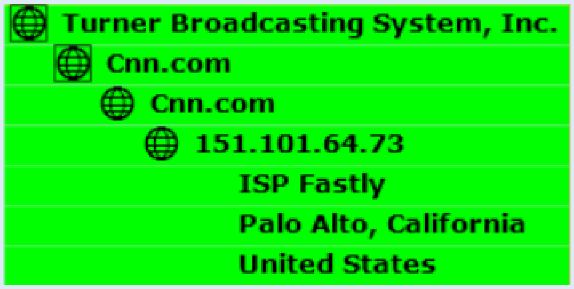
Controlling Browser Traffic

Drilling Down

The best way to understand Hacker Deterrent's internal organization is to drill down on any entity. To drill down:

- Right-Click any Entity to reveal all the Domains underneath.
- Right-Click any Domain to reveal the Sites underneath
- Right-Click any Site to reveal the IP Addresses underneath
- Right-Click any IP Address to get the Geolocation underneath

Consider the following example:



Turner Broadcasting System, Inc.
Cnn.com
Cnn.com
151.101.64.73
ISP Fastly
Palo Alto, California
United States

Just right-click on each item again to collapse it.

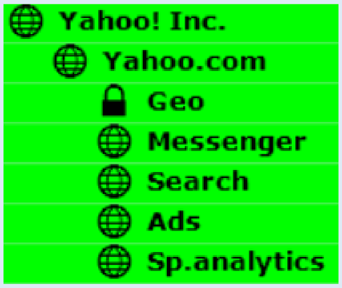
Blocking/Allowing

To toggle blocking/allowing, simply left click on any name.

- The 🌐 symbol indicates *allowed traffic*.
- The 🔒 symbol indicates *blocked traffic*.

You can block/allow based on Entity, Domain, Site, or IP Address. This gives you complete flexibility to control all the traffic flowing in and out of your computer.

Consider the following example:



Yahoo! Inc.

Yahoo.com

Geo

Messenger

Search

Ads

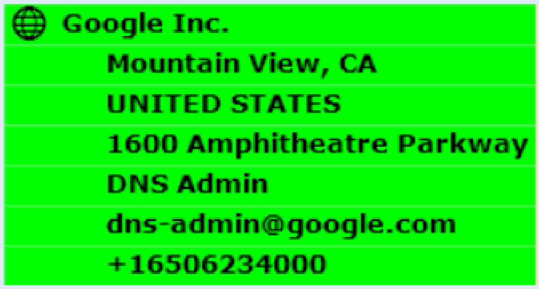
Sp.analytics

In this example, all traffic to the Entity Yahoo! Inc is allowed except for one site on the domain Yahoo.com: **geo**.yahoo.com. This site is blocked while everything else remains allowed. This is an example of how much control you finally have over your traffic.

Detailed Entity Info

To see detailed information on any entity, <Ctrl> Right-Click on the entity name.

Consider the following example:



Google Inc.

Mountain View, CA

UNITED STATES

1600 Amphitheatre Parkway

DNS Admin

dns-admin@google.com

+16506234000

To collapse the Detailed Entity Info, <Ctrl> Right-Click the Entity name again.

Color-Coded Reputations

Hacker Deterrent automatically checks the reputation of every Site that your browser wants to connect. Hacker Deterrent displays the reputations via the following color-code:

- Green: Known Reputable
- Red: Known Malicious
- Yellow: Unknown Reputation

Two important notes regarding color-coding:

- Red sites are automatically blocked. You always have the freedom to unblock them. But do so with extreme caution.
- On occasion, two sites owned by an entity may have different reputations. In this situation, you will see the Entity name twice. For example, if EntityA-Site1 has a green reputation but EntityA-Site2 has a yellow reputation then you will see the name of Entity A in both the green and yellow areas. You can drill down to see which Sites have the individual reputation.

Controlling Application Traffic

Note: In this User Guide, the word *application* will be used to refer to every software program other than your *browsers*.

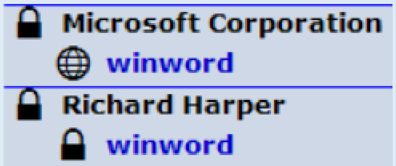
Blocking/Allowing

All application traffic is initially blocked. All you have to do is left-click on any application to allow it to talk to the Entity which it's under.

Application blocking/allowing uses the following symbols:

- The 🔒 symbol indicates *blocked traffic*.
- The 🌐 symbol indicates *allowed traffic*.

Consider the following example:



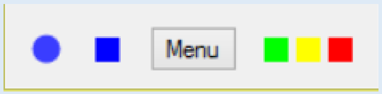
🔒 Microsoft Corporation
    🌐 winword
🔒 Richard Harper
    🔒 winword

In this example, the application "winword" is allowed to talk to Microsoft Corporation However, it's being blocked from talking to a site owned by Richard Harper.

For maximum security, just follow one simple rule: **Only allow apps to talk to their makers.** For example, only allow "winword" to talk to Microsoft since Microsoft is its maker. If all your apps solely talk to their makers then none of your apps can be used for piggybacked communication to hackers. It's truly that simple.

Health Monitor and Controls

In “Control Mode” you will see the following at the bottom of Hacker Deterrent:



The blue circle is the Health Monitor. It is continually monitoring the health and integrity of the Hacker Deterrent traffic controller. As long as the circle is blue and blinking, Health Monitor has determined that Hacker Deterrent’s traffic controller is functioning properly. If the circle either changes color or stops blinking, ***disconnect from the internet immediately***. Either situation indicates that malware is directly attacking the integrity of Hacker Deterrent. Health Monitor is another unique feature of Hacker Deterrent, to help you achieve maximum protection against hackers.

The colored squares are your control buttons. They filter traffic, making it even easier for you to watch whatever you’d like to focus on:

- Green Square: Filters green, *allowed* browser traffic.
- Yellow Square: Filters yellow, *allowed* browser traffic.
- Red Square: Filters red, *allowed* browser traffic.

You will notice that *blocked* browser traffic is always displayed, regardless of the filter settings. Therefore, if you’ve accidentally blocked something that a website needs to function, you can easily see the error and fix it with a single click. You never need to worry about accidentally blocking anything, because it can always be easily undone.

The blue square switches Hacker Deterrent between two Modes:

- Control Mode: Shows all browser traffic and all app traffic.
- Monitor Mode: Solely shows the names of browser who are actively talking, and solely shows the names of Entities who are talking to internet-based applications.

Monitor Mode is most useful when you aren’t using your browser but need extra screen space when using other applications. It will allow you to keep an eye out on Health Monitor as well as see the names of everyone accessing your computer. However, the window is much smaller than Control Mode, leaving you plenty of screen space to use your applications.