# Table of Contents

**Overview** ................................................................................................................................. 1  
Best Practice #1: Cybersecurity Defense in Depth ................................................................. 2  
**MalBlock Configuration Best Practices** .................................................................................. 4  
Best Practice #2: Web Filters ........................................................................................................ 4  
Best Practice #3: Malware and Phishing Protection ............................................................... 4  
Best Practice #4: Web Content Filtering .................................................................................... 6  
Best Practice #5: Scheduled Reports .......................................................................................... 7  
**DNS Security Hardening – Network Firewall Rule** ............................................................... 9  
**Infected Device Identification** ................................................................................................ 10  
MalBlock Standard - Infected Device Identification ............................................................... 12  
MalBlock Premium - Infected Device Identification ............................................................... 14  
Client ID Device Tracking .......................................................................................................... 14  
**Threat Remediation** .................................................................................................................... 16  
Ransomware .............................................................................................................................. 16  
Microsoft Windows, Mac OS, Chromebook, Android and iOS .............................................. 16  
Internet of Things (IoT) .............................................................................................................. 17
Overview

This application note describes how MalBlock DNS Security fits into your overall security posture, best practice recommendations and guidance for identifying and remediating malware infected devices.

MalBlock operates by blocking DNS lookups from network clients to malicious domains and websites on the Internet to break the cyberthreat attack chain:

Figure 1. How DNS Breaks the Cyberthreat Attack Chain

MalBlock is a Defense-in-Depth network perimeter security that protects everything in the network including computers, servers, Point of Sale terminals and Internet of Things (IoT) such as cameras, printers, routers and thermostats and building automation controls:

Figure 2. MalBlock DNS Security: Defense in Depth
**Best Practice #1: Cybersecurity Defense in Depth**

No single solution can protect against all threat vectors because malware can be introduced behind the network perimeter and no solution can guarantee absolute security. A best practice is to implement all the protections in **Error! Reference source not found.** for a defense in depth strategy. However, this requires planning, time, budget and technical skills. Businesses with a tighter budget and more limited resources should address the areas outlined below. They are listed in order of priority.

1. **MalBlock Security**
   
   Malware, ransomware, phishing and botnets use DNS for survivability and to evade detection. With nothing to install, MalBlock protects everything behind the office Internet connection including computers, servers, routers and IoT devices where anti-virus software is not supported.

2. **Anti-Virus Endpoint Protection**
   
   Install anti-virus/malware endpoint protection software on all computers, tablets and smartphones. Cox Business includes McAfee anti-virus with your Cox Internet subscription. Endpoint protection is extremely important because:
   
   - It travels with the device.
   - Most Internet traffic is encrypted for secure communications. Network firewalls are often blind to encrypted traffic and therefore cannot block threats. However, the traffic is always decrypted by the endpoint at which stage it can be scanned by the anti-virus software.

3. **Data Backup: 3-2-1 Rule**
   
   Restore from a data backup is often the only way to recover from a ransomware attack or other catastrophes such as fire or flood. The 3-2-1 Rule is easy to remember and is a proven data backup strategy recommend by the United States Computer Emergency Response Team (US-CERT). The rule is:
   
   - Keep three (3) copies of your data: One (1) primary and two (2) backups.
   - Use two (2) different types of media, for example:
     - Secondary internal hard drives, network drives or removeable drives.
     - Cloud storage such as Google Drive, Microsoft OneDrive, DropBox, etc.
   - Keep one (1) copy offsite.
   - Prevent loss of backups if the business location suffers a catastrophe such as theft, fire, flood or wind damage.
   
   **Tip:** In addition to file and folder backups, consider using disk image backup software such that the entire operating system, applications, and data can be restored in a single step.
4. **Vulnerability Patching / Upgrades**

Enable automatic upgrades and patching on Linux, Windows and Mac OS systems to fix known vulnerabilities. Remember to upgrade the software on your router and switches. IoT devices are especially vulnerable. Check the manufacturer’s website for firmware or software upgrades. Also be sure to change the router or IoT device default username and password because cyber criminals scan for default credentials.

5. **Network Firewall**

A network firewall is recommended to block internal and external threats, in addition to allowing only company sanctioned applications, monitoring and reporting. Cox Business offers Managed Router and Security to fulfill this need.
MalBlock Configuration Best Practices

The following settings should be enabled for maximum protections via the MalBlock web portal. You can access the portal by signing into https://myaccount.coxbusiness.com.

**Best Practice #2: Web Filters**

The Web Filters (Global URL Protection) setting determines if Web Content Filtering and user-defined “Block and Allow Lists” are enforced.

The Web Filters On/Off control is located at the top-right corner of the portal. It is set to ON by default when your account is created. (Note: A warning message appears if Web Filters are OFF. See Figure 3.)

**Best Practice #3: Malware and Phishing Protection**

Malware, Phishing and Botnet protection are enabled by default.

Use the following steps to access the Internet Security screen.

1. Login to the web portal.
2. From the main screen, navigate to Settings → Protection Preferences, and scroll down to Internet Security. (Important: Malware and Phishing Protection should be turned ON.)
Consider enabling Google SafeSearch, Bing SafeSearch and YouTube Restricted Mode to filter adult content in online searches. MalBlock supports this by resolving the safe/restricted domain if the DNS lookup is for the standard domain:

- bing.com ➤ strict.bing.com
- google.com ➤ forcesafesearch.google.com
- youtube.com ➤ restrict.youtube.com
Best Practice #4: Web Content Filtering

Web Content Filtering is available with MalBlock Premium and blocks websites based on approximately 60 categories. One-click filter presets for None, Light, Medium, Strict and Custom are available for quick setup.

A good practice is to select the Medium (or Strict if desired) filter preset. Both filter types include the following high risk (malware and infected download) categories:

- **Anonymizer**: Sites that facilitate anonymous surfing.
- **Download Sites**: Sites that contain downloadable software, whether shareware, freeware, or for a charge. Includes some peer-to-peer sites.
- **Hacking**: Sites that promote or give advice about how to gain unauthorized access to proprietary computer systems.
- **Illegal Software**: Sites that illegally distribute software or copyrighted materials.
- **Peer-to-Peer**: Sites that enable direct exchange of files between users without dependence on a central server.
- **Pornography/Sexually Explicit**: Sites that contain explicit sexual content.

Figure 5. Web Content Filtering

Use the following steps to access the Web Filters screen.

1. Login to the web portal.
2. From the main screen, navigate to Settings → Protection Preferences, and scroll down to Web Filters.
Best Practice #5: Scheduled Reports

Use the Scheduled Reports feature to receive specific data on a pre-defined timeframe.

Figure 6. Configure Scheduled Reports

Use the following steps to schedule reports and have them emailed to you on a specified timeframe.

1. From the Scheduled Reports screen, enter your Email address and select the Frequency for which you want them sent: Daily, Weekly or Monthly. Result: An email will be sent summarizing block events. (Note: If you do not want reports sent to you, select Never in the Frequency drop-down menu.)

2. Click the Manage Settings button in the report to access the MalBlock dashboard and investigate suspicious activity. (See Figure 7.)
Figure 7. **Scheduled Report Sample**

From: Dir_Not_Reply_Staging (CC: Atlanta) <CN5.Staging@mail.cox.com>
Sent: Monday, July 15, 2019 9:56 AM
To: [Email]
Subject: Cox Business MalBlock Service Monthly Summary Report

Cox Business MalBlock Service

Account Name: **Acme Products**

Here's your security summary for the last month.

108372
GLOBAL URL FILTER BLOCKS

90
PHISHING & MALWARE BLOCKED

20
BOTNET BLOCKED

© 2019 Cox Communications, Inc. All rights reserved.
DNS Security Hardening – Network Firewall Rule

MalBlock Security is cloud-based solution that blocks malicious domains including malware, phishing and botnets. A brief system overview is illustrated in Figure 8. The high-level operation is:

- **Step 1**: DNS lookups are processed by the MalBlock DNS Servers. If a domain is malicious or matches a web content filter, it is blocked and the session ends.
- **Step 2**: If the domain is not blocked, the IP address for the requested domain/website is returned to the LAN client and the Internet Request proceeds.

![MalBlock Network Overview](image)

Figure 8. MalBlock Network Overview

Protctions and restrictions are enforced only if LAN devices send their DNS lookups to the MalBlock DNS Servers. Devices with hard-coded or misconfigured DNS settings and DNS hijacker malware infected clients will bypass MalBlock.

A best practice is to deploy a network firewall with a DNS Security policy that **blocks all Internet traffic on port 53 with a destination IP address that does not match the MalBlock servers**. Port 53 is the standard port for DNS. Policy violations will be displayed in the firewall traffic logs for investigation.

For quick reference the MalBlock DNS Server IP addresses are:

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>72.200.254.11</td>
<td>2001:57a:102::11</td>
</tr>
<tr>
<td>72.200.255.11</td>
<td>2001:57a:103::11</td>
</tr>
</tbody>
</table>
Infected Device Identification

Cox Business regularly review existing and new threats on the Internet, taking swift action to block malware, phishing, and botnet attacks at the DNS level. The data science team updates the Threat List every day. As a result, new threats may already be blocked before our business customers are made aware.

Identifying malware infected devices is critical to prevent an infection from spreading and to begin remediation (cleaning the infection). The identification process will depend on your MalBlock configuration and device inventory records.

This sections reviews the MalBlock (standard) Dashboard and describes the types of blocks that are covered.

- **Global URL Filter Blocks** are benign and the result of user-defined Web Content Filters and Block & Allow Lists.

- **Malware & Phishing Blocks** are high risk events and should be investigated via **See More** button (shown below) to view event logs.

- **Botnet Blocks** are a severe risk and represents machine-to-machine traffic between an infected device (zombie) and a Command & Control server. Click the **See More** button for event logs.

  Note: The full Threat List contains hundreds of entries.

The Dashboard provides a summary of the types and number of blocks that MalBlock has identified.

**Figure 9. MalBlock Standard Dashboard**
Use the following steps to access the Malware & Phishing Event Log.

1. Login to the Portal.
2. From the main page, click the See More button in Figure 9.

A sample Malware & Phishing blocked event log is shown in Figure 10. The Reason column description will display “Infected page” for malware or “Phishing page” for phishing domains. These types of events are primarily the result of interactive human activity, such as browsing the web or clicking a phishing link in an email.

**Figure 10. Malware & Phishing Event Log**

<table>
<thead>
<tr>
<th>URL</th>
<th>Reason</th>
<th>Device Name/ID</th>
<th>Time Period</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.ms69-hinet.net/favicon.ico">http://www.ms69-hinet.net/favicon.ico</a></td>
<td>Infected page</td>
<td>Unknown</td>
<td>Sep 30, 2019 06:00 pm - 06:15 pm</td>
<td>1</td>
</tr>
<tr>
<td><a href="http://www.ms69-hinet.net/">http://www.ms69-hinet.net/</a></td>
<td>Infected page</td>
<td>Unknown</td>
<td>Sep 30, 2019 06:00 pm - 06:15 pm</td>
<td>1</td>
</tr>
<tr>
<td><a href="http://drumbaseuk.com/">http://drumbaseuk.com/</a></td>
<td>Infected page</td>
<td>Unknown</td>
<td>Sep 30, 2019 05:45 pm - 06:00 pm</td>
<td>1</td>
</tr>
<tr>
<td><a href="http://chrom-update.online/favicon.ico">http://chrom-update.online/favicon.ico</a></td>
<td>Infected page</td>
<td>Unknown</td>
<td>Sep 30, 2019 05:45 pm - 06:00 pm</td>
<td>1</td>
</tr>
<tr>
<td><a href="http://drumbaseuk.com/favicon.ico">http://drumbaseuk.com/favicon.ico</a></td>
<td>Infected page</td>
<td>Unknown</td>
<td>Sep 30, 2019 05:45 pm - 06:00 pm</td>
<td>1</td>
</tr>
<tr>
<td><a href="http://chrom-update.online/">http://chrom-update.online/</a></td>
<td>Infected page</td>
<td>Unknown</td>
<td>Sep 30, 2019 05:45 pm - 06:00 pm</td>
<td>1</td>
</tr>
</tbody>
</table>

The Botnet Event Log displays the Threat Type to better identify the malware.

**Figure 11. Botnet Event Log**

<table>
<thead>
<tr>
<th>URL</th>
<th>Threat Type</th>
<th>Device Name/ID</th>
<th>Time Period</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>talkfonflyatlanti.org</td>
<td>Zeus</td>
<td>Unknown</td>
<td>Sep 30, 2019 11:30 am - 11:45 am</td>
<td>17</td>
</tr>
<tr>
<td>sytes.net</td>
<td>Zeus</td>
<td>Unknown</td>
<td>Sep 30, 2019 11:30 am - 11:45 am</td>
<td>328</td>
</tr>
<tr>
<td>sytes.net</td>
<td>Zeus</td>
<td>Unknown</td>
<td>Sep 30, 2019 10:45 am - 11:00 am</td>
<td>2</td>
</tr>
</tbody>
</table>

When you click the name of the Threat Type in the Botnet Event Log; e.g., Zeus, the list of threat descriptions for that type appear in the Online Help screen.

**Figure 12. Zeus Botnet Threat List**

Zeus is a Trojan/virus that records usernames/passwords and other sensitive data, transmits them to malicious sites over the Internet, and can allow unrestricted remote access to infected computers. Details: Microsoft

Zitmo is an Android and Blackberry variant of the Zeus family of financial-fraud malware. Zitmo is short for “Zeus in the Mobile.”
Infected device identification with MalBlock Standard is an indirect process because Device Name/ID (MAC address) tracking is not supported by the Standard tier.

Use the following steps to identify or eliminate infected devices include:

1. Observe the dashboard graph in Figure 9
   
   a. Are the blocked events regularly occurring 24x7? If so, the device is “always on” such as a server, router, IP camera, printer or other IoT device.
   
   b. Do the blocks happen occasionally, perhaps during normal working hours? If yes, it's probably due to an employee browsing the web, reading e-mails and other human activities.
2. Click the **See More** button in Figure 9 to view the event logs. (See Figure 10 and Figure 11).
   a. Are the same URLs repeated blocked?
   b. What is the Reason (Malware & Phishing) or Threat Type (Botnet)? (Note: Knowing the Reason/Threat Type is critical to determine the appropriate steps to resolve.)
   c. Do the events occur during working hours (1st shift, 2nd shift, etc.) or diminish in volume when certain employee(s) are not in the office? If so, it can narrow the search by focusing on desktops, laptops or mobile devices used by those persons.

3. Shutdown or disconnect devices one-at-a-time from the network.
   a. For Mobile Devices, disable WiFi on the device.
   b. For Wired Devices, unplug the Ethernet cable, either from the device or at the switch/router port serving the device.

4. Wait 30 minutes and check the dashboard counters and event logs.
   a. Do the blocked events stop or drop in volume (more than one device may be compromised)? If yes, then that device is likely infected.

5. If you have a network firewall, check the firewall traffic logs for the URLs in the blocked event logs. The firewall logs contain the LAN client/device source IP address that attempted to reach the blocked site.

6. Once the infected device(s) is identified, keep it disconnected from the network to isolate and prevent further damage.
MalBlock Premium - Infected Device Identification

MalBlock is sold as a tiered subscription, Standard and Premium. MalBlock Premium has advanced features to identify infected devices by Client ID (MAC Address & Device Name). If Client ID is not enabled, follow the MalBlock Standard processes in the MalBlock Standard - Infected Device Identification section.

Client ID Device Tracking

MalBlock Premium requires dnsmasq configuration, a free, lightweight DNS forwarder on a customer-owned router or small Linux server to enable Client ID tracking. See the Dnsmasq Configuration Guide for Ubuntu Desktop for instructions.

When the Client ID is enabled with dnsmasq, the MAC address of the LAN client/device is included with DNS lookups. MalBlock automatically adds new devices to the “New Devices (Unsaved)” default Group. New devices should be given an easily recognizable name and assigned to different Groups for unique protections and restrictions. (See Figure 14.)

![MalBlock Premium: Device Inventory](image)

1. Click the See More button, shown on Figure 9, below the dashboard counters to view the blocked event logs and Device Name/ID.
The event log identifies the “Dell XPS 8920 Desktop” computer was blocked when it tried to access the malicious site citicards[.]cm because the user mistakenly entered .cm instead of .com for the real site “citicards.com.”

2. Click the Export raw data button to download the full event log in .CSV format or save the file.

Botnet infected devices should be disconnected from the network to prevent further damage. Botnet blocking counters can be quite large and represents a persistent infection. Every effort should be taken to remediate a botnet.
Threat Remediation

MalBlock is a *prevention* service that blocks DNS lookups for malicious domains and websites. It cannot remove a malware infection, but it can block communications with Command & Control (C&C) servers to halt its progress. For example, preventing ransomware from “phoning home” to a C&C server to download encryption keys.

Remediation actions vary based on the malware family and device type. The best approach is to engage the services of a cybersecurity professional. Cox Business Complete Care – IT Support for Small Business can provide remote assistance to remove viruses, malware and spyware.

Alternatively, basic self-remediation steps may be viable. The following are general guidelines. *(Note: Success is not guaranteed and the user assumes all risks.)*

The remediation process varies by the malware and device type as outlined in the following sections.

**Ransomware**

Ransomware encrypts files and displays a notice demanding payment in cryptocurrency (e.g. Bitcoin) to receive the decryption keys for unlocking the files. Removing the ransomware infection will not work because your files remain encrypted. Paying the ransom is not advised and there’s no guarantee you will receive the keys. Some ransomware strains always destroy files even if the ransom is paid.

The surest ransomware recovery method is to erase the disk drive, reinstall the operating system and restore files from a backup copy. See the Threat Remediation section for data backup best practices.

**Microsoft Windows, Mac OS, Chromebook, Android and iOS**

Run a full anti-virus scan on the PC. If you do not have anti-virus endpoint protection software installed, a free version may be available from the following companies¹ or other software vendors.

- [McAfee](#) for Windows PC is included with your Cox Business Internet subscription.
- [MalwareBytes](#) supports Windows, Mac OS, Chromebook, Android and iOS.
- [AVG](#) – Windows PC, Windows Server, Mac OS and Adroid
- [Avast](#) supports Windows PC, Windows Server, Mac OS and Linux.

If malware is detected, follow the quarantine/removal instructions provided by the anti-virus software.

---

¹This does not constitute or imply a company endorsement by Cox Business.
Internet of Things (IoT)

IoT devices such as routers, cameras, printers, thermostats, and video conferencing systems are especially vulnerable to compromise because:

- Factory default login credentials are often never changed.
- Firmware/software vulnerabilities known as Common Vulnerabilities and Exposures (CVE) are actively exploited by criminals.
- IoT devices are often unmanaged.
- Devices may have limited manufacturer support. Upgrades and patches may not be available.

The general remediation steps for a compromised IoT device are:

1. Check the manufacturer’s website for firmware/software upgrades, release notes and security advisories. If an advisory is available, follow those instructions.
2. Download any firmware/software updates.
3. Reset the device to factory defaults.
4. Install the firmware/software upgrade if available.
5. Change the factory default username and password. (Tip: The username should not be ‘admin’ and the password should be strong.)
6. Configure the device for your requirements.
7. The DNS Primary and Secondary Server settings should be set to **Automatically Obtain via DHCP (preferred)** or set them to the MalBlock DNS Server IP addresses as noted in the **DNS Security Hardening – Network Firewall Rule** section.

End of Document