Malware Prevention With Barracuda Content Shield

https://campus.barracuda.com/doc/94539462/

Note that the Malware Prevention feature (MPC) was no longer sold as part of BCS Plus after December 21, 2021. If you purchased your subscription before that date, and if you installed the MPC agent on endpoint machines, then this article applies.

If you have a *BCS Plus* subscription, you have access to the Malware Prevention Component (MPC) included in the BCS agent for Windows endpoints. The MPC provides file-based security with several levels of risk analysis, including:

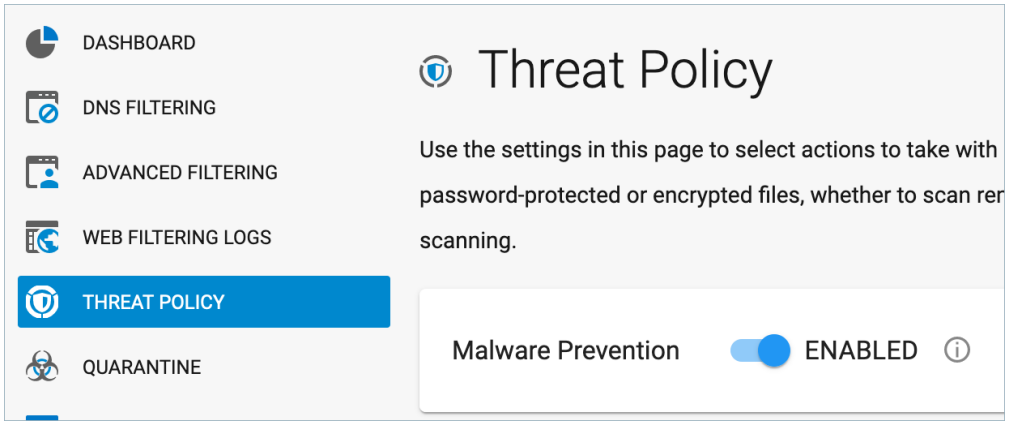
- Checking against known malware signatures
- Static file analysis
- Dynamic thread analysis

Note that the MPC is disabled by default as described below. This article discusses the features of the MPC; to configure, see How to Set Threat Policies.

Threat policies are configured on the **THREAT POLICY** page to specify how you want to handle files determined to be *clean*, *suspicious*, or *malicious*.

- A file is deemed *suspicious* if the file has certain attributes associated with malware, but the scanner cannot make an absolute determination. For example, the scanner cannot access a password-protected or encrypted file, and therefore cannot determine if the file is a real threat. If a **7z** format archive is opened or extracted by the user, then the scanner can access the files and detect and block threats.
- A file is *malicious* if Barracuda Content Shield has scanned the file and has designated that file as a threat that should not be accessed by users. **Malicious files (on local drives) are removed. On network and removable drives, they are not removed, but blocked from opening or executing.**
- A file is *clean* if no malicious or suspicious indicators were found by any scanners.

You can enable the MPC by setting **Malware Prevention** to *Enabled* on the **THREAT POLICY** page.



Important: The MPC is disabled by default because the endpoint machine may appear to experience some latency while the MPC scanner performs an initial scan on the endpoint drive(s). Knowing this allows the administrator to prepare users for this potential latency when the MPC is first enabled, perhaps enabling the feature during off-peak work hours.

If **Malware Prevention** is disabled on the **THREAT POLICY** page, threat policies will *not* be applied on the endpoint machines. The **Status** tab on the BCS interface on the clients will show *Content Protection Disabled.* Web content filtering will still apply to web traffic per policy.

When the Malware Prevention Scanner Runs on the Endpoint

When enabled, threat policies you configure on the **THREAT POLICY** page sync with endpoint machines running the BCS agent every 5 minutes, and the file scanner runs on the client machine:

- Upon installation, performing a full system scan
- Whenever the user accesses or downloads a file
- Based on the (optional) frequency you configure using the **Schedule Full Scan** setting (on the **THREAT POLICY** page)

Files Excluded From Scanning

Files can be excluded from or exempt from scanning based on policies you set in BCS

- Process exclusions (on-access scanner only) as configured on the EXEMPTION POLICIES page.
- Path or file name exclusions as configured on the **THREAT POLICY** page.
- File type exemptions (e.g. Microsoft Office files, PDFs, executables) configured on the **THREAT POLICY** page.

Note that the MPC does not support scanning RDS User Profile Disks on Windows Server systems.

Scheduling Scans

You can either run a scan immediately by clicking **RUN NOW** on the **THREAT POLICY** page, or click **SCHEDULE** to set a regular scan schedule for endpoints. See How to Set Threat Policies for details.

Figures

© Barracuda Networks Inc., 2022 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.