

CIGENT WINDOWS FOR SEAGATE® BARRACUDA™ 515 SSD

USER GUIDE v1.0



September 2024 V1 Seagate® BarraCuda™ 515 Cigent Windows Version 5.0.6 **SEAGATE**

🐞 BARRACUDA

515 Series M.2 NVMe SSD

)

Contents

| Introduct | ion | 3 |
|-----------|--|-----|
| Purpose | | . 3 |
| Setup an | d Installation | . 4 |
| Com | patibility with Cigent PBA software | . 4 |
| Quick Sta | rt Wizard | . 6 |
| Understa | nding Invisible vs Visible Drive state | . 9 |
| Understa | nding Always vs During Threat protection | 10 |
| Understa | nding threat sensors and their impact | 13 |
| BarraCud | a 515 SSD Advanced Features | 18 |
| 1.1 | Erase Verify | 18 |
| 1.2 | KeepAlive | 20 |
| 1.3 | Command Log | 24 |

Introduction

The BarraCuda[™] 515 SSD operating firmware includes cybersecurity defenses that repel ransomware attacks and data theft — even when all other cybersecurity protections fail. In conjunction with Cigent Windows software (Cigent), BarraCuda[™] 515 SSDs protect data throughout the entire device lifecycle—from provisioning to end-of-life—defending against a vast number of threat vectors.

BarraCuda 515 SSDs can be installed as the primary storage device on a Windows PC where the O/S runs, as secondary internal storage (such as in a desktop tower) or as external media plugged into a USB port.

Cigent is a new approach to data security, one that complements existing solutions and places the importance of protecting data above all else. Cigent takes concepts used in threat containment and continuous authentication and applies them as close to the data stream as possible, bringing proactive protection directly to your data. Cigent allows users to safely and easily access critically important information, even if the system is already compromised. The result is an unprecedented level of protection, detection, and response to cyberattacks, insider threats, and lost or stolen devices.

Purpose

This document is a guide to help you install and configure your BarraCuda 515 SSD and associated Cigent Windows software so you can start using it as quickly as possible. It also provides a basic operation overview and explanation for some of the security sensors if you are interested in learning more.

Setup and Installation

This guide is applicable to Seagate BarraCuda 515 SSDs installed internally as primary or secondary drives or externally.

Compatibility with Cigent PBA software

Cigent Windows software can be used on systems with or without Cigent PBA software, however there are some requirements and differences when used together. The main requirements and differences are listed below and will also be noted throughout the guide.

- 1. Cigent PBA software must be installed before installing Cigent Windows software.
- 2. Authentication for Secure Drive operations (creation, deletion and unlocking) uses Cigent PBA credentials instead of Cigent Windows authentication.
- 3. Creation and deletion of Secure Drives requires a Cigent PBA administrator account.

A copy of the Cigent Windows installer is placed onto each Seagate BarraCuda 515 SSD before shipping.

The latest versions of Cigent software can always be found at https://www.cigent.com/support/seagate

| Double click the EXE to start the installation. | ^ + C □ > This PC > Local Disk (C) > Installer Image: C Image: C Image: C > Installer Image: C Image: C Image: C Image: C Image: C Image: C Image: C Image: C Image: C Image: C | |
|---|---|---|
| | | Name Date modified Type Size |
| | | Chata_Defense_Installer_v4.0.9.exe 3/5/2024 5:37 PM Application 73,773 KB |
| | | Data_Defense_Installer_v4.0.9.msi 3/5/2024 5:37 PM Windows Installer 66,059 KB |
| 2. | Select Yes on the User Account Control popup. | User Account Control X Do you want to allow this app to make changes to your device? Control Data Defense Verified publisher: CIGENT TECHNOLOGY, INC. File origin: Hard drive on this computer Show more details. |
| | | |



Quick Start Wizard

| 1. | Shortly after the installation completes, a setup wizard will appear that will guide the user through basic setup of a Secure Drive (if present) and folder protection. Click Setup standalone to begin. | K Cet started Setup with my business subscription Betup stantig |
|----|--|---|
| 2. | If discovered, the setup wizard | ≰cigent × |
| | will present an option to configure a single secure drive. | Your drive has been detected |
| | | Cigent Secure SSD |
| | Enter a password twice and click Confirm. | Secure your drive This passnerd protects the drive in the case of theft or if the operating system resets. Confirm your password to proceed with quick drive set up. You can also configure with additional settings later in the Secure drive tab. |
| | | Back Continue without seared drive Confer |
| 3. | Accept or change the Secure drive size. | SciceNT × Your drive has been detected |
| | Change the Protection mode to | Q Cigent Secure SSD |
| | NOT be During threats. This results in an Always secure drive | Secure drive size |
| | which will be used for this tutorial. | The Smount of drive space being reserved as a secure drive 83.3 GB (recommended) Protection mode |
| | Click Confirm. | During threats (recommended) Authentication is only required when threats are detected. You Can change this later in Settings. |
| | | Back |

| <u> </u> |
|----------|
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |



CONGRATULATIONS

You have completed the steps necessary to begin using your BarraCuda 515 SSD and Cigent Windows software.

If you want to learn more about how to use your BarraCuda 515 SSD and Cigent proceed further in this guide.

Understanding Invisible vs Visible Drive state

The first layer of data protection we will cover is invisible data. The secure drive you just created is special in that it can be either visible or invisible to the operating system. When invisible, all data stored on the drive is protected from threats like ransomware, malware and even malicious insiders simply because it cannot be accessed. To gain access to data on the drive, users can manually make the drive visible using step up authentication. As an additional layer of protection, secure drives will also automatically become invisible if a threat is detected. (More on this later.)

When a secure drive is invisible the drive appears to the OS as a small read only partition containing only a convenient program (unlock.exe) to make the drive visible. When visible, the full drive appears to the OS exposing all data stored on the drive. The drive letter remains the same in both states.

 Open Windows Disk Management, Windows Explorer and Data Defense as shown.



 Click the toggle icon to change the drive to Visible. Notice how the partition appears in Disk Management and Explorer and you can now see your data.

Understanding Always vs During Threat protection

Each type of data protection including secure drive, folder and file type in Data Defense supports two modes, Always and During Threats. End users or administrators can choose the option that best suits the level of protection based on the type of data being protected.

During Threats protection only requires step up authentication to access protected files when the threat state of the endpoint is elevated. The threat state can become elevated by an internal Data Defense sensor or by an externally integrated source. The standalone version of Data Defense has a Trusted Network and Anti-virus sensor. If a sensor detects a potential threat, users must authenticate each file access until the threat is remediated.

Always protection requires step up authentication to access protected files every time by default. The File Reauthentication Frequency setting allows changing the access authentication to occur after a predetermined number of accesses over a period of time. This greatly reduces the impact on the user of accessing protected files while balancing the risk of unauthorized access.

The use of Always protection and File Reauthentication Frequency is the recommended mode of protection by Cigent.

In this section we will start interacting with files to see the file protection in action. You can either use some of your own files or you can download the files used in this guide.

https://cigent.blob.core.windows.net/download/SampleFiles.zip

| 1. | Create a folder C:\temp and copy SampleFiles.zip into it. Right click to Extract All. files. Change location to C:\temp. When complete, you should have a HighlyConfidential folder in C:\temp. | This PC This PC Local Disk (C:) Installer Intel PerfLogs Program Files Program Files (x86) temp HighlyConfig^{Im}tial SampleFiles.zip | Name Annual Report - draft - confidential.docx billing.xlsx Confidential Level1.docx Confidential Level2.docx Confidential Level3.docx Confidential Level4.docx Confidential Level5.docx fw4.pdf k fw4.pdf k iw9.pdf k iw9.pdf |
|----|---|---|--|
| | | > 🤤 Users > 🔭 Windows > 🌾 Always On (unlocked) (L: > 🐲 Network | :) i) mlb.pdf ii) nfl.pdf j pgaMasters.pdf |
| 2. | Make sure your Always On Secure Drive is Visible and the copy the HighlyConfidential folder to L:\. | | Name Source Lock.exe HighlyConfidential |
| 3. | Open Data Defense -> Settings. Change the File Reauthentication Frequency to 2. The changes the requirement to authenticate from every time to every third time. | CICENT DASHBOARD DRIVES Settings C File Reauthentication Freque C The number of protected file acc specified time per authentication | FOLDERS & (3) noy esses over the 2 Files by the B Hours |

| 4. | In Windows Explorer, navigate to L:\HighlyConfidential. Double- click to open Confidential Level1.docx. Since this is the first file being opened today, authorization is required. Notice the name of the file and requesting application is indicated letting the user know what is accessing the particular file. | HoppCathened X + |
|----|--|--|
| 5. | Enter your credential and the file will open. | Image: Conducted land door : NumPer Image: Cond door : NumPer |
| 6. | Double click on Confidential Level2.docx. Notice the file opens without authentication. This is because you set the reauthentication frequency greater than zero. | Image: Section of the section of this document's format. Some content might be set of the section of the secti |
| 7. | You can see how many pre- authenticated file access you have left by right clicking on the Data Defense tray icon. | Sign In View Dashboard View Settings Clear Alert Remaining auths: 1 |

8. Open Confidential Level3.docx (a) × and then open Confidential Windows Security Name Level4.docx. Upon attempting to Annual Data Defense[™] open Confidential Level4.docx, billing.x Authorization is required to allow access of "Confidential Level4.docx". you are again required to Confide By: Windows Wordpad Application authenticate because you had Confide Confide no remaining precigent Confide 2 authentications. Password Confide DESKTOP-T1K4HMV\cigent A fw4.pdf A fw9.pdf More choices 🛃 iw9.pdf Mib.pd OK Cancel 🔊 nba.pdf A nfl.pdf

Understanding threat sensors and their impact

As mentioned earlier, the threat state of Data Defense is determined by its sensors. These sensors are either internal or external. The standalone version of Data Defense has two sensors available, Trusted Network and Anti-virus tethering. Additional sensors are available with the Data Defense subscription and are not covered in this guide.

The Trusted Networks sensor (inactive by default) looks for connections to newly connected networks and increases the threat level of Data Defense until the user trusts the network. This can occur if a user joins an open wifi network at a coffee shop for example. Users can also not trust a network leaving the threat state elevated for increased file protection.

The Anti-Virus tethering sensor monitors the state and status of the active anti-virus application in Windows. If the anti-virus program detects a virus or becomes disabled, Data Defense with elevate the threat level.

When the threat level is elevated by a sensor, the following occurs:

- 1. Always On secure drives are automatically made invisible.
- 2. During Threat secure drives are conditionally locked based on the settings in Data Defense.
- 3. The Remaining pre-authentication count is reset to zero.

4. Files on During Threat secure drives or in During Threats folders will require authentication for each file access.

In the follow section, we will trigger the Data Defense Anti-virus sensor to see the effect.

| 1. | Open files on the Always On secure drive so you have at least 1 pre- authentication remaining. | | Sign In View Dashboard View Settings Clear Alert Remaining auths: 1 |
|----|---|----------------|---|
| 2. | We will assume Windows Defender is the active | Wind | dows Security - No actions needed. |
| | anti-virus. If you are using something else, you should be able to accomplish the same but the steps will vary. Open Windows Security control by clicking the tray icon. | | 🍯 🚳 🍕 🕃 🗇 d× 📾 |
| 3. | Click Virus & threat | Window | vs Security |
| | protection | 4 | |
| | | \equiv | Security at a glance |
| | | 6 | See what's happening with the security and and take any actions needed. |
| | | 0 | |
| | | 8 (r) [] | Virus & threat protection No action needed. |

| 4. Select Manage settings | Windows Security C Virus & threat protection Protection for your device against threats. C Current threats Last scan: 5/14/2024 12:21 PM (quick scan) 0 threat(s) found. Scan lasted 52 seconds 29657 files scanned. Quick scan Scan options Allowed threats Protection history |
|---|--|
| | 🗞 Virus & threat protection settings |
| | No action needed. Manage settings |
| | |
| 5. Click on the toggle to turn off the real-time protection | windows security ← = ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ |
| | B Real-time protection Locates and stops malware from installing or running or can turn off this setting for a short time before it turns I automatically. Image: Constraint of the setting for a short time before it turns I automatically. Image: Constraint of the setting for a short time before it turns I automatically. Image: Constraint of the setting for a short time before it turns I automatically. Image: Constraint of the setting for a short time before it turns I automatically. |
| 6. Select Yes. | User Account Control X Do you want to allow this app to make changes to your device? Windows Security Verified publisher: Microsoft Windows Publisher Show more details Ves No |

7. Return to the Data CIGENT × Defense dashboard on DASHBOARD DRIVES FOLDERS 9 ŝ notice the red banner Microsoft Defender Antivirus seems to be disabled indicating the elevated This alert is generated when Microsoft Defender Antivirus appears to be disabled or its signatures are out of date. You cannot clear this alert, however you can disable the antivirus status check by disabling the 'Anti-Virus Tethering' sensor from the Sensor page. threat state due to the Antivirus sensor. Secure drives Θ Sensors Trusted Network Also notice that the NVISIBLE Cigent Secur.. 83.99 GB - Always 0 > Always On secure drive is Anti-Virus Tethering Threat detected > now locked (safeguarding Protected folders the files on the drive.) X Protected folders Э Upgrade your account to get more sensor protection O Data Deception Removable Storage O Network Deception Upgrade to get more protection - Local Disk (L:) × + → ↑ C 💭 > This PC > Local Disk (L:) D New - 🔏 🕼 🛅 🙆 🖻 🕥 🛝 Sort ~ 🗮 View ~ 🚥 Name Date modified Type ↓ Downloads 7/12/2023 4:04 PM Unlock.exe Application Documents Local Disk (C) - Local Disk (L:) tighlyConfidential 🚞 temp 8. Notice the Data Defense Sign In tray icon is now red View Dashboard indicating an active threat. **View Settings** Right click on the icon and also notice the remaining auths is reset to 0. Remaining auths: 0 9. Re-enable the real-time Windows Security protection. 6 🗞 Virus & threat protecti = View and update Virus & threat protection set Antivirus. G O **Real-time protection** 8 Locates and stops malware from installing or ((q)) can turn off this setting for a short time befor automatically. O On 2 -



BarraCuda 515 SSD Advanced Features

So far, we have covered the first three layers of data protection provided by Data Defense when combined with a supported SED to create Secure Drives.

- 1. Invisible data
- 2. Step up authentication
- 3. Threat sensors and response

Although these protections are strong, they are primarily enabled in software which a sophisticated adversary could attempt to bypass or find a vulnerability. For example, should a threat actor gain administrative control of the host, they could disable Data Defense and its components. If the secure drive was currently unlocked, the data would be accessible.

That is where the Cigent firmware enhancements come into play to close those threat vectors. The three firmware features available in the Barracuda 515 SSD are:

- 1. Erasure Verification
- 2. Keep-Alive heartbeat
- 3. Command Log

Next we will examine and test each of these features to get an understanding of how they work.

1.1 Erase Verify

Secure data erasure is an important process for many commercial and governmental organizations preventing classified information from unauthorized access. Short of costly and wasteful physical destruction, users had to depend on outdated erasure programs originally written for magnetic media. Solid State Drives require different methods of erasure to prevent recovery by today's advanced tools and technique. Barracuda 515 SSDs support extended erasure verification commands to check each and every mapped and unmapped block to verify the data has been removed. Any blocks reporting data will result in an erasure verification failure. Once Data Defense confirms the drive has been truly erased, it can be safely and securely reused.



If you have questions on how best to accomplish complete data erasure, please contact Cigent support for some guidance.

1.2 KeepAlive

KeepAlive provides an extra layer of protection by creating a tighter trust connection between the firmware (SSD) and the software (Data Defense). When enabled, a non-replayable heartbeat continuously plays between Data Defense and the Barracuda 515 SSD such that if the drive fails to receive the proper response in time, the drives will automatically lock. This prevents any chance a hacker could stop Data Defense protection once a drive is unlocked. This makes it impossible to access the files on the Barracuda 515 SSD without Data Defense running.

KeepAlive was automatically setup and enabled when you configured your Secure Drive. Indication it is enabled can be seen on the secure drive panel:



Since Windows caches a significant amount of file and directory information, testing Keepalive can be a bit of a challenge just using windows explorer. The best method is using a simple batch script to continuously write a test file to the secure drive and then stop the Data Defense service. After about 30 seconds the script will no longer be able to write to the secure drive because the firmware automatically locked it.

d, it will eventually fail to create new files.

| 1. | Ensure the Secure Drive is unlocked. | This PC Name | |
|----|---------------------------------------|---|---|
| | | Lock.exe | Education |
| | | installer ingniscon | ndenuar |
| | | Intel | |
| | | PertLogs | |
| | | > Program Files | |
| | | > Program Files (X80) | |
| | | v internet | • |
| | | Seconda Siles eine | |
| | | > campieriles.zip | |
| | |) Uindowr | |
| | | Always On (unlocked) (L:) | |
| | | HighlyConfidential | |
| | | 📬 Network | |
| | | | |
| 2 | Open Services application and | 😪 Services File Action View Help | - 🗆 X |
| ۷. | locate the Cigent service | | |
| | locate the cigent service. | Ggent Name Description | Status Startup Type Los ^ |
| | | Description: Calibration Control Contr | o Running Manual (Tig Loi 1 Running Automatic Loi 1 Manual Ne |
| | | Capability Access Manager Provide for Capability Access Manager Provide for Capability Access Manager Capability Access | c Running Manual Lor ii Manual Lor w Running Manual Lor |
| | | Christer Propagation Copies und | M. Kunning Automatic Loi Menual (Trig., Loi Manual (Trig., Loi Russian Automatic Loi |
| | | Client Licence Service (ClipS Provides int CNG Key Isolation The CNG ke | f Manual (Trig., Lor s., Running Menuel (Trig., Lor |
| 3. | Right-Click on the row and select | Cigent Properties (Local Computer) | × |
| | Properties. Change all of the failure | General Log On Recovery Dependencies | |
| | actions to "Take No Action" then | Select the computer's response if this service fails. He | lp me set up recovery |
| | click ok. | First failure: Take No Action | ~ |
| | | Second failure: Take No Action | ~ |
| | | Subsequent failures: Take No Action | ~ |
| | | Reset fail count after: 0 days | |
| | | Restart service after: 0 minutes | |
| | | Enable actions for stops with errors. | omputer Options |
| | | - Run program | anglassi alpaninisti |
| | | Program | |
| | | | Browse |
| | | Command line parameters: | |
| | | Append fail count to end of command line (/fail- | =%1%) |
| | | | |
| | | OK Ca | ancel Apply |
| 4. | Create a batch file called | keepalivetest.bat × | + |
| | keepalivetest.bat on your C: drive | File Edit View | |
| | with the following contents: | echo off | |
| | č | echo "This is a test" >> test.txt | |
| | | :start copy test.txt L: /v | |
| | | timeout 5 | |
| | | Bara start | |
| | | | |

| 5. | Open a command prompt (Administrator) and run batch file and leave it running | <pre>Administrator Command Prompt - keepalivetest.bat C:\Users\cigent\Desktop>keepalivetest.bat C:\Users\cigent\Desktop>echo off 1 file(s) copied. Waiting for 0 seconds, press a key to continue 1 file(s) copied. Waiting for 5 seconds, press a key to continue</pre> |
|----|--|--|
| 6. | Open another command prompt(Administrator) and run the command 'taskkill /f /IM cigentservice.exe' to forcibly shutdown the Cigent Service. | Administrator.Command Prompt Microsoft Windows [Version 10.0.22631.3447] (c) Microsoft Corporation. All rights reserved. c: \Windows\System32>taskkill /f /im cigentservice.exe SUCCESS: The process "CigentService.exe" with PID 13324 has been terminated. C: \Windows\System32> |
| 7. | Notice that soon the writes begin to fail. This is an indication that the keepalive timed out and the firmware locked the drive. Windows explorer may not even notice the drive is locked until you attempt to access it but eventually it will. | <pre>Maministrator: Command Prompt- keepalivetertLast 1 file(s) copied. Waiting for 0 seconds, press a key to continue 1 file(s) copied. Waiting for 0 seconds, press a key to continue 1 file(s) copied. Waiting for 0 seconds, press a key to continue 1 file(s) copied. Waiting for 0 seconds, press a key to continue 1 file(s) copied. Waiting for 0 seconds, press a key to continue 1 file(s) copied. Waiting for 0 seconds, press a key to continue 1 file(s) copied. Waiting for 0 seconds, press a key to continue Access is denied. 0 file(s) copied. Waiting for 0 seconds, press a key to continue Access is denied. 0 file(s) copied. Waiting for 0 seconds, press a key to continue Access is denied. 0 file(s) copied. Waiting for 0 seconds, press a key to continue Access is denied. 0 file(s) copied. Waiting for 0 seconds, press a key to continue Access is denied. 0 file(s) copied. Waiting for 0 seconds, press a key to continue Access is denied. 0 file(s) copied. Waiting for 0 seconds, press a key to continue Access is denied. 0 file(s) copied. Waiting for 0 seconds, press a key to continue Access is denied. 0 file(s) copied. Waiting for 5 seconds, press a key to continue</pre> |
| 0 | Postart the service using services | Ggert Properties (Local Computer) X Ggert Properties (Local Computer) X |
| 0. | Restart the service using services | General Log On Recovery Dependencies 2 General Log On Recovery Dependencies |
| | and reset the failure actions to | Service name: operataavoo ********************************** |
| | restart service. | Path to executable: Subsequent failure: Pertart the Service U |
| | | Statup type: Automatic V I Restat fail court after: 0 days I Restat senice after: 1 minutes 1 |
| | | Catalor a for stops with emms. Restart Computer Options Service status: Running Run program |
| | | Start D. Stop Pixee Resure You can specify the dat parameters that apply when you dant the service from here. |
| | | Start parameter: |
| | | OK Cancel Apply OK Cancel Apply |
| 9. | Unlock the Always On drive using | [33] Administator Command Prompt - keepalewisetstat Naiting for 6 seconds, press a key 60 continue The system cannot find the drive specified. |
| | Data Defense. (Note, you may have | Waiting for θ seconds, press a key to continue \ldots The system cannot find the drive specified. |
| | to lock and unlock the drive twice | Waiting for 0 seconds, press a key to continue The system cannot find the drive specified. |
| | to return the drive to its previous | positing for 8 seconds, press a key to continue The system cannot find the drive specified Maiting for 8 seconds, press a key to continue |
| | drive letter (L:) | The system cannot find the drive specified. Waiting for 0 seconds, press a key to continue |
| | Notice that after unlocking the | The system cannot find the drive specified. Waiting for 0 seconds, press a key to continue The system cannot find the drive specified. |
| | drive, the script is once again able | Waiting for 0 seconds, press a key to continue The media is write protected. |
| | to write to the secure drive. | ating for 8 seconds, press a key to continue |
| | | Maiting for 8 Secundo, panes a kay to continue |

| 10. Terminate the batch file using | |
|------------------------------------|--|
| Control-C. | |

1.3 Command Log

Barracuda 515 SSDs automatically store every command sent to the drive in a tamperproof location in memory on the drive. Cigent Data Defense also periodically writes markers to the log to indicate the activity was performed with Data Defense running and that the activity was properly authorized. Commands are stored for all partitions including unsecured locations (for example the C: drive.)

This command log can be used to audit drive activity to capture attempts to read information from the drive without Data Defense possibly indicating attempts to circumvent file protection. Further, the command log can be used to report on files accessed with or without Data Defense running by mapping the accessed locations to the current file system layout. This can reveal important information to investigators attempting to understand what was accessed or at least attempted to be accessed.

Retrieving the command log would normally only be done during a forensic investigation or to understand if a drive has been tampered with.

| 1. | In Data Defense->Drives, select Command Log. | Secure drives Protect files with firmware locking, the highest level of protection |
|--|--|--|
| | | Cigent Secure SSD IOSJ IOSJ тоти. szz sni pw Modify 894.25 G8 SP1210729001000006 ECFM13.3 Remove |
| | | Secure drive (L:) Protection Mode Show in File Explorer Always Protection Mode Show in File Explorer Erase Verify |
| 2. Select Scan. NOT can take 30 minu can always stop t click Stop. Any da to that point will | Select Scan. NOTE: This process can take 30 minutes or more. You can always stop the process by click Stop. Any data retrieved up | DASHBOARD DRIVES FOLDERS & Stop |
| | to that point will be viewable. | Affected File Report Generate File reports are based on file locations at the generated time From 05/14/2024 • 12:00 AM • To 05/14/2024 • 12:00 AM • From 05/14/2024 • 12:00 AM • To 05/14/2024 • 12:00 AM • Unauthorized Date / Time Authorized Unauthorized Start End Read Write |

| 3. Eventually, you will start to see | Retrieving command logs, this may take a while |
|---|---|
| rows start appearing in the table | Command log audit Full Rescan Scan |
| starting with the oldest dates | Affected File Report Generate |
| available. | File reports are based on file locations at the generated time |
| Once data is displayed, you can | From 04/29/2024 💙 04:21 PM 🗘 To 04/30/2024 🌱 04:06 PM 🗘 |
| stop the retrieval, but it is | Date / Time Authorized Unauthorized Start End Read Write Read Write |
| suggested you wait until it is | 4/29/2024 4/29/2024 796281 464350 3437117 1487386 |
| suggested you wait until it is | 4/29/2024 4/29/2024 1052276 273588 5175124 2061948 |
| complete to see data from your | 4/30/2024 4/30/2024 520965 149931 310672 /3620 4/30/2024 4/30/2024 11653 76545 133730 60446 |
| previous activities as a result of | 4/30/2024 4/30/2024 236040 757568 0 0 |
| following this guide. | |
| 4. Once complete a popup will | |
| annear Click Ok | |
| | DASHBOARD DRIVES FOLDERS 2 191 |
| | + Second Second Second Second |
| | Command log audit turkuur tur |
| | Affected file Report |
| | The reports are based or the second sec |
| | Command log processing complete |
| | OK INTERNET |
| | 4/25/0014 4/21 PM 64580 3407117 4/25/0014 6/25 PM 4/25/0024 6/20 PM 105/276 275686 6/75124 |
| | AURICIDITA TALIK ANT AURICIDIA TALIK MAR SLIDBED VERSIT 310072 |
| | 42802024 534 PM 42902024 638 PM 11955 7645 152730 42802024 431 PM 42902024 439 PM 28102202 4945278 7756972 |
| | 4/8520254 530 PM/ 4/852024 538 PM/ 2018 72947 4611224 |
| C Conclute the and of the table and | |
| 5. Scroll to the end of the table and | <pre></pre> <pre><</pre> |
| select a row that encompasses | DASHBOARD DRIVES FOLDERS 일 (양 |
| the times during which you were | Return to Secure drives |
| following this guide. Then click | Command log audit Full Rescan Scan |
| Generate. | Affected File Report File reports are based on file locations at the generated time |
| | From 05/14/2024 V 01:00 PM 🗘 To 05/14/2024 V 01:59 PM 🗘 |
| | Date / Time Authorized Unau Start End Read Write Read |
| | 5/14/2024 9:20 AM 5/14/2024 9:59 AM 4/94815 520783/ 0 5/14/2024 10:00 AM 5/14/2024 10:26 AM 21004 243308 97474 |
| | 5/14/2024 12:06 PM 5/14/2024 12:59 PM 40016390 28137721 84106 5/14/2024 1:00 TV 5/14/2024 1:59 PM 284892 131060 174849 |
| | 5/14/2024 2:00 PM 5/14/2024 2:59 PM 1462373 448948 0 5/14/2024 3:00 PM 5/14/2024 3:59 PM 133723 2130893 91155 |
| | |
| Click Save after choosing the | save report to X ↔ → ↑ → Documents |
| report location and name. | Organize ▼ New folder |
| | > OneDrive Name Date modified Type Size |
| You will be asked to authenticate | No items match your search. |
| To a win be asked to authenticate | ± Downloads ≉ |
| | Documents # H Local Disk (C) |
| | 🐇 Always On (unk |
| | File name (20 yen) Secure SSD 20220514 1300-20220514 1559.cvv |
| | Save as type 1 cov |
| | A Hide Folders |

| 7. Data Defense will then process the command long and cross reference the file system with the access blocked to create an affected file report. | CLIGENT X DASHBOARD DRIVES FOLDERS 2 3 Careerating command log report Command log audit Full Resear Scan Affected File Report Generated time File reports are based on file locations at the generated time |
|---|---|
| 8. Click Ok | Command Log Report Generated |
| 9. Find and open the file ending in csv_files.csv. | Cigent Secure SSD_20240514_1300-20240514_1359.csv_files.csv |
| Search the file for "Level1". Hopefully you will see an entry for the file used during this evaluation. | Exemptiveteritatist Cigent Secure SSD_20240514_1300 × File Edit View MSEDGEEWERVENDL CKS-2029F30pf ; Yes; {d833f5c5-53d9-46bd-b15d-4e7729c6e23f}; C, 113789, 180433, 1, 2024-05124, 0, 6367.207_124, 0, 637.207_124, 0, 637.207_124, 0, 637.207_124, 0, 637.207_124, 0, 637.207_124, 0, 637.207_124, 0, 637.207_124, 0, 637.207_124, 0, 637.207_124, 0, 637.207_124, 0, 637.207_124, 0, 637.207_124, 0, 637.207_124, 0, 637.207_124, 0, 67.207_ |

Authorized activities occurred while Data Defense was running. Unauthorized activities occurred without Data Defense running which can be during system start up or perhaps if the drive was accessed from another system while in an external enclosure. It does not necessarily mean the activity was malicious but can give clues as to how it was accessed.

For more information about Seagate BarraCuda 515 SSDs please visit ww.seagate.com

©2022 Cigent Technology Inc. All rights reserved. Cigent is a registered trademark of Cigent Technology Inc. in the United States and other jurisdictions. Seagate is a registered trademark of Seagate Technology LLC in the United States and/or other countries. BarraCuda is either trademark or registered trademark of Seagate Technology LLC or one of its affiliated companies in the United States and/or other countries.