STEALTHbits TECHNOLOGIES

CCSI

DATA SHEET

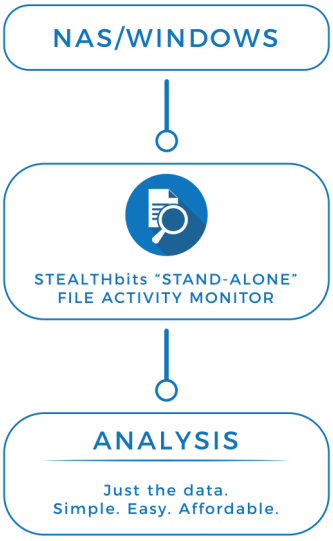
STEALTHbits File Activity Monitor

KNOW WHEN EVERYTHING HAPPENS IN YOUR FILE SYSTEMS

The ability to monitor file access activity across file shares residing on NAS and Windows devices represents both a tremendous gap and opportunity for organizations looking to identify threats, achieve compliance, and streamline operations.

Unfortunately, many organizations can't answer basic questions around data activity, often for these reasons:

1. The volume of data is typically more than organizations can handle with manual auditing.
2. Native logging introduces massive performance issues.
3. Native logging, once enabled, can quickly fill up file system logs with noise, and offers no effective means by which to search for answers.
4. For NAS devices specifically, native auditing is often so difficult to configure that most organizations don't bother
5. File Activity Monitoring technologies are often buried within larger solution suites, making them cost prohibitive.



BENEFITS

The STEALTHbits File Activity Monitor is a simple-to-install, easy-to-use solution that monitors and stores file activity for NAS (NetApp, EMC, Hitachi) and Windows devices. The solution is designed to provide users with the ability to:

1. Query all file activity for specific values or combinations of values
2. View query results executed against your data in a clean, simple UI grid
3. Feed file activity data to alternative technologies like SIEM (Splunk and QRadar) and/or export data in easy-to-understand and use formats
4. Analyze data feed into SIEM to gain insight into overall file activity, deletions, modifications, critical permission changes, and file system attacks like ransomware.

SIEM SOLUTION:

- Resolve SID to AD user display name
- Filter on each grid column
- Sort each column in the grid
- Display row count
- See status bar
- Know what query was run

PRESENT QUERY DATA IN A GRID:

- Resolve SID to AD user display name
- Filter on each grid column
- Sort each column in the grid
- Display row count
- See status bar
- Know what query was run

COLLECT & EXECUTE QUERIES ON:

- Date and date ranges
- Hosts
- User who performed the action
- The file/folder path affected by the action

REPORTING DATA TARGETS:

- CSV
- PDF
- SIEM

DATA SHEET

HOW IT WORKS

The STEALTHbits File Activity Monitor is an agent-based file activity monitoring solution. Agents are deployed to Windows server endpoints and NAS activity is collected by agents deployed to Windows proxy servers that leverage deep integration with NetApp, EMC, and Hitachi.

SUPPORTED PLATFORMS AND EVENT COLLECTION

Windows and NAS CIFS/NFS Events (Windows, NetApp, EMC, Hitachi)		
• File Create • File Delete • File Open • File Rename • File Modify • File Change Permissions	• Folder Create • Folder Delete • Folder Rename • Folder Change Permissions • Folder Change Ownership	• Access Denied – File Open • Access Denied – File Delete • Access Denied – File Set Permissions • Access Denied – Folder Delete • Access Denied – Folder Change Permissions • Access Denied – Folder Change Ownership *Windows Only

SYSTEM REQUIREMENTS

Management Console

- Windows Server 2008+
- .NET 4
- Minimum 2 GB of dedicated RAM

Agent

- NET 4
- Minimum 1 GB dedicated RAM per file monitoring service (Windows, EMC, NetApp, HNAS are separate services)

*Storage requirements depends on rate of customer activity. One event = ~1kb of storage.

STEALTHbits TECHNOLOGIES

STEALTHbits Technologies is a cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data.