DATA SHEET

STEALTHBITS FILE ACTIVITY MONITOR

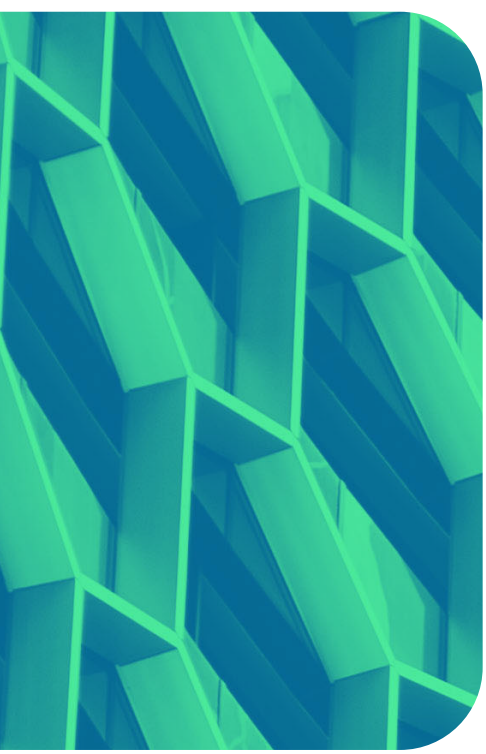
Features, capabilities, and use cases

Understanding activity means understanding risk, compliance stature, and the opportunity for cost reduction – common, yet highly desirable ideals for any business. However, many organizations never fully harness the power of data because they have trouble enabling and tuning activity auditing within standard repositories like Windows or NAS platforms and SharePoint.

Not only do organizations struggle to obtain activity data from critical systems, they also aren't gathering activity across their infrastructure because of the:

- Cumbersome nature of native logging
- Costs associated with aggregating and storing data
- Complexity of understanding the data.

Stealthbits enables organizations to capture activity efficiently across the entire organization and multiple platforms, as well as effectively derive meaningful insight from the activity to address security, compliance, and operational requirements. The result is an organization that understands the answers to critical data security questions at a moment's notice like:



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:

- Surface threats and events in a single view
- Identify Crypto Ransomware attacks
- Identify data access vulnerabilities as they occur
- Quickly resolve malicious or accidental file deletions
- Analyze file activity and user authentications

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

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)

NEXT STEPS

Schedule a Demo

stealthbits.com/demo

Download a Free Trial

stealthbits.com/free-trial

Contact Us

info@stealthbits.com

IDENTIFY THREATS. SECURE DATA. REDUCE RISK.

Stealthbits Technologies, Inc. is a customer-driven cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, our highly innovative and infinitely flexible platform delivers real protection that reduces security risk, fulfills compliance requirements, and decreases operational expense.