DATA SHEET

STEALTHBITS ACTIVITY MONITOR

Activity Auditing Made Easy

Native audit logs are noisy, kludgey, performance intensive, and often void of the details and context administrators need to address security and compliance use cases with certainty and ease. Logs of activities occurring within popular file system and storage platforms, on-premises and cloud-based services like SharePoint and Microsoft 365 SharePoint Online, and directories like Active Directory and Azure Active Directory are particularly difficult to make heads or tails of and are overly verbose, resulting in a serious lack of visibility into the two most important resources within any organization: credentials and data.

Stealthbits Activity Monitor acts as an embedded component of multiple Stealthbits products but can also be licensed and leveraged as a stand-alone solution to drastically ease the burden activity auditing places on your organization's people, processes, and technologies.

BENEFITS

High-Fidelity, Streamlined Activity Auditing

Stealthbits Activity Monitor intelligently monitors and interprets activities, translating event output into information that both humans and computers can understand.

Simple, Straightforward Reporting

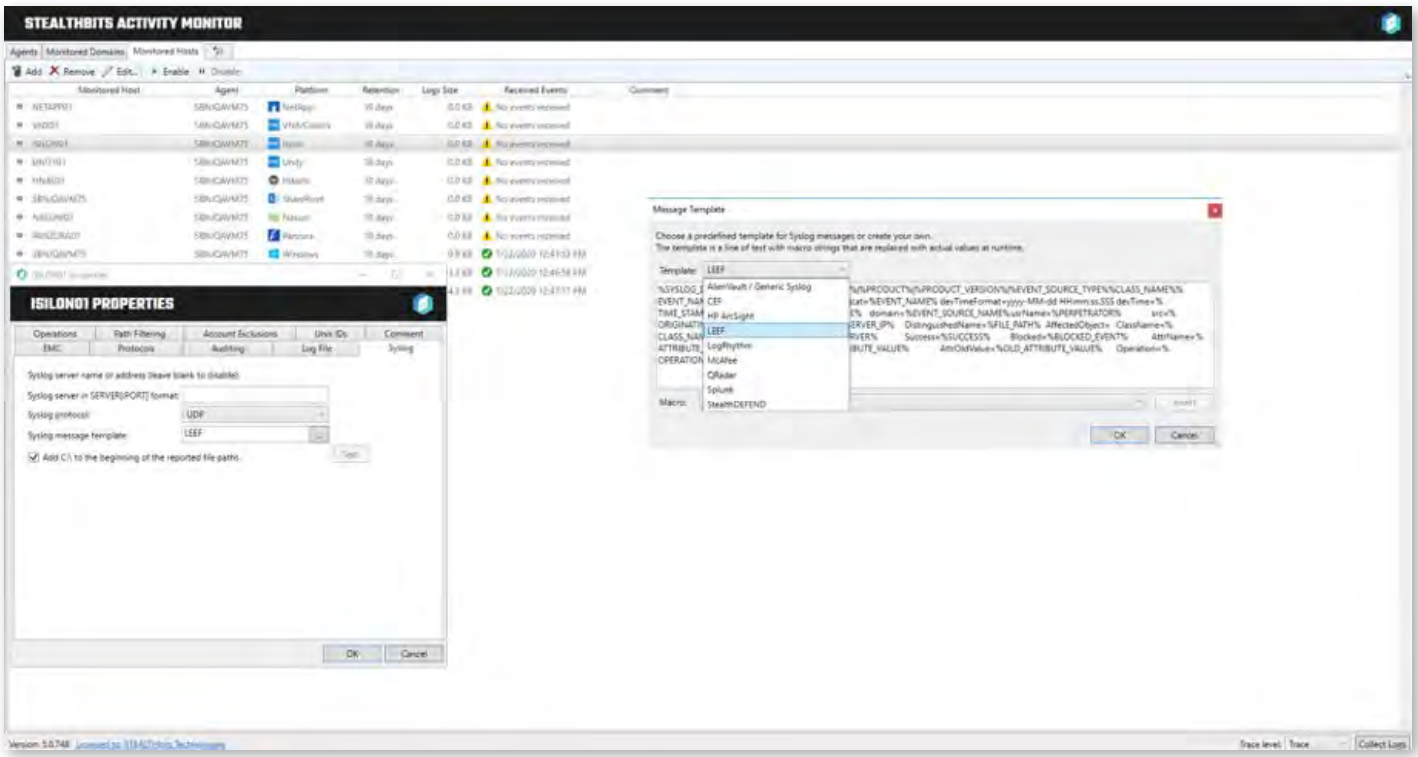
With easy to use output filtration and sorting options, users can answer simple and complex questions rapidly and without a PhD in data analytics.

Flexibility and Interoperability

It's your data, so Stealthbits Activity Monitor provides the facilities you need to use it however and send it wherever you want.

How It Works

The Stealthbits Activity Monitor is an agent-based activity monitoring solution. In real-time, Stealthbits Activity Monitor audits, records, and optionally hosts or sends high-fidelity, streamlined activity information to whatever needs it, including SIEM platforms like Splunk and LogRhythm, reporting tools like Tableau and Power BI, IAM and IGA platforms, and more.



Supported Platforms and Event Collection

Windows and NAS CIFS/NFS Events (Windows, NetApp, DellEMC, Hitachi, Nasuni, Panzura)

EVENTS		
File Create	Folder Create	Share Create*
File Delete	Folder Delete	Share Delete*
File Read	Folder List	Share Update*
File Rename	Folder Rename	Share Permission Changes*
File Modify	Folder Change Permissions	
File Change Permissions	Folder Change Ownership	

*For Windows NTFS Only

Additional capabilities include:

- Access Denied for all events can be reported*
- Smart office filtering: removes much of the noise of user actions which allows admins to focus on the user activity over raw file I/O for 3 major versions of Office
- For Windows: monitoring for creation and access to shadow volumes

SHAREPOINT

OPERATIONS		
Check-Out	Check-in	View
Search	Update	Copy
Move	Child Move	Delete
Undelete	Audit Mask Change	File Fragment Write
Profile Change	Schema Change	Workflow
Custom		

PERMISSION OPERATIONS		
Creation of a user group	Deletion of a group	Addition of a new member to a group
Deletion of a member from a group	Creation of a new role	Deletion of a role
Changing a role	Turning off inheritance of a role	Changing permissions of a user or group
Turning on inheritance of security settings	Turning off inheritance of security settings	Deletion of audit events
Granting App permissions	Revoking App permissions	

M365 SharePoint Online

Over 150 events in the following categories:

CATEGORIES		
File and Page	Folder	List
Share and Access Requests	Site Permissions	Site Administration
Synchronization	DLP	Sensitivity Label
Content Explorer	Other	

Active Directory

- Active Directory Change Monitoring - Report any successful and/or failed attempt to change AD objects or attributes for the following operations:
- Added, Deleted, Modified, Moved or Renamed
- Authentication Monitor – report success and fail for Kerberos and/or NTLM authentications
- LDAP Monitor with filters for success/fail, servers, users, host-from, LDAPQuery string to match, LDAP result string to match
- LSASS Guardian - reports attempts by other programs to inject into LSASS
- AD Replication Monitor - reports an event if a non-listed machine (not joined to the Domain) attempts to act as a replication partner

Azure Active Directory

- Reports Sign-In events
- Reports over 800 Audits events in different categories and across different services:

CATEGORIES		
Administrative Unit	Application Management	Authentication
Authorization	Authorization Policy	Contact
Device	Device Configuration	Directory Management
Entitlement Management	Group Management	Identity Protection
Kerberos Domain	Key Management	Label
Permission Grant Policy	Policy	Policy Management
Resource Management	Role Management	User Management

SERVICES		
AAD Management UX	Access Reviews	Account Provisioning
Application Proxy	Authentication Methods	B2C
Conditional Access	Core Directory	Device Registration Service
Entitlement Management	Hybrid Authentication	Identity Protection
Invited Users	MIM Service	MyApps
PIM	Self-service Group Management	Self-service Password Management
Terms Of Use		

- Send Event Data to SIEM, StealthDEFEND, StealthAUDIT, or Syslog
- Stores searchable activity data with a configurable retention interval

System Requirements

Management Console

- .NET 4.6.1
- Minimum 2 GB of dedicated RAM

Agent

- .NET 4.6.1
- Minimum 1 GB dedicated RAM per file monitoring service (Windows, EMC, NetApp, HNAS are separate services)
- Windows Server2008R2 and Above

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.