Data Sheet

StealthINTERCEPT®

Change & Access Auditing | Real-Time Alerting

Monitor & Enforce Security Policy

StealthINTERCEPT is a real-time change and access monitoring solution that safeguards your organization against malicious and unintended changes made in Active Directory, File Systems, and Exchange. By monitoring these changes at the source, StealthINTERCEPT generates security and operational intelligence in real-time without relying on ineffective native logs.

Noisy, Irrelevant Data Prevents Action

For years, organizations have struggled to obtain contextual, actionable intelligence from their critical Microsoft infrastructure to address security, compliance, and operational requirements. Even after pumping SIEM and other log aggregation technologies with every event possible, critical details are lost amidst excessive amounts of noise or are too difficult to interpret for administrators to make heads or tails of what is really happening in their environments. As bad actors continue to leverage more and more sophisticated methods to elude detection, the need for a new way to analyze changes and activities for violation of security and operational policies is paramount to detecting and preventing an inevitable breach.

Cut Through the Noise

By intercepting all traffic without any reliance on native logging, StealthINTERCEPT is able to identify authentication-based and file system attacks, monitor usage and abuse of privileged accounts, and detect critical changes made to the environment. Furthermore, StealthINTERCEPT is capable of instantiating preventative controls that lock down your most critical assets and actually enforce the written policies of which there are no effective technical controls. Together, these capabilities enable the visibility and protection you've needed for years, but could never previously obtain using native utilities or third-party products.

Key Benefits:

- **Policy Enforcement** – Prevent the changes and activities that put your organization at risk
- **Increased Security** – Unprecedented insight into user behavior and changes taking place in your environment to identify internal threats.
- **Simplified Audit & Compliance** – Automate the generation of critical compliance artifacts in alignment with industry and regulatory standards.
- **Empowered SIEM** – Correlate threat data providing crucial context about attack techniques and behaviors without the need for native logs.
- **Preventative controls** – Increase security posture and reduce operational risk by preventing critical changes and inappropriate access.
- **Complete Event Details** – Comprehensive event details for every event improves visibility and context, making data more actionable.

Features

Attack Analytics – Built-in authentication and file system analytics allow organizations to catch and automatically block internal threats as they're unfolding using customizable, pattern-based detection techniques.

Reconnaissance Detection – Reconnaissance is the first phase of every targeted attack. StealthINTERCEPT's ability to surgically monitor LDAP requests against Active Directory enables real-time detection of suspicious queries such as the membership of privileged security groups and the location of sensitive assets.

In-line Monitoring – StealthINTERCEPT eliminates reliance on native logs through in-line monitoring of events. By intercepting event details at the source, organizations get better data, faster, and more efficiently than native logging can provide.

Change & Access Prevention – Add an additional layer of security and control to your Active Directory, File System, and Exchange environments through integrated blocking capabilities at the finest levels, including AD objects and GPOs, authentications, files, and mailboxes.

Real-Time Alerting – StealthINTERCEPT will alert any audience of your choosing to critical events in real-time at global or policy-specific levels.

True SIEM Integration – So much more than just a syslog feed, StealthINTERCEPT provides direct, certified integration with many of the market's leading SIEM technologies, including IBM® QRadar®, Splunk, RSA® Security Analytics, and HP® ArcSight®. Events feed in real-time, formatted and parsed properly out of the box, along with rich pre-packaged dashboards that provide a complete, ready-to-use experience.

Dynamic Policies – Leverage existing security investments to dynamically enrich the context of StealthINTERCEPT policies, such as a list of critical security groups to monitor for membership changes or privileged accounts to monitor for unauthorized authentications.

Powerful Investigations – StealthINTERCEPT's Investigation Grid provides users with easy access to the Who? What? Where? When?™ of any event, including before and after values, complete originating and destination IP Addresses and Host Names, and more. Any investigation can also be saved for one-click viewing in the future from the console or the web.

Extensible Actions – Administrators can save time and add advanced actions using the easy automation and scripting functionality provided by PowerShell, VB, and C#.

Role-based Access – Whether in the console itself or via StealthINTERCEPT Web Reporting interfaces, the controls are there to ensure the right people have access to only the right product components and data, saving time and ensuring security for administrators, auditors, and other data viewers.

Integrated Security – StealthINTERCEPT not only protects your critical assets, but itself as well by generating a tamper-proof audit trail of all activities performed inside the product, hardening deployed agents, and ensuring compatibility with embedded OS security features like FIPS.

Integrated Reporting – From the console or the web, users can take advantage of StealthINTERCEPT's Investigations Grid, Analytics, and Reporting facilities.

Supported Platforms

Active Directory	File Systems	Exchange

Windows Server 2008 32-bit
Windows Server 2008 64-bit
Windows Server 2008 R2 64-bit
Windows Server 2012
Windows Server 2012 R2
	Windows:
	• Windows Server 2008 32-bit
	• Windows Server 2008 64-bit
	• Windows Server 2008 R2 64-bit
	• Windows Server 2012
	• Windows Server 2012 R2
	• Windows Server 2016
	
	NetApp:
	• ONTAP 7.2+ (7-Mode and Cluster -Mode)
	
	EMC:
	• EMC Celerra 6.0+
	• EMC VNX:
	  • VNX 7.1
	  • VNX 8.1
	• EMC VMAX3
	• EMC Isilon devices:
	  • Isilon 7.0
	  • Isilon 7.1
	  • Isilon 7.2
	
	Hitachi:
	• Hitachi 11.2+
		Exchange Server 2010
		Exchange Server 2013
		Exchange Server 2016

About STEALTHbits Technologies

STEALTHbits Technologies is a cybersecurity software company focused on protecting an organization's credentials and data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, we reduce security risk, fulfill compliance requirements and decrease operations expense.

Identify threats. Secure data. Reduce risk.

STEALTHbits Technologies, Inc.
200 Central Avenue
Hawthorne, NJ 07506 USA
P: +1.201.447.9300 | F: +1.201.447.1818
sales@stealthbits.com | support@stealthbits.com
www.stealthbits.com