Data Sheet

StealthINTERCEPT

Real-Time Change Monitoring & Threat Detection

Real-time Security Intelligence

StealthINTERCEPT is a real-time change monitoring and threat detection solution that safeguards your organization against malicious and unintended changes made in Active Directory, Exchange, and File Systems. By monitoring these changes at the source, StealthINTERCEPT generates security 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. 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 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 attacks, monitor privileged accounts, and detect changes made to the environment. Furthermore, StealthINTERCEPT is capable of instantiating preventative controls that lock down your most critical assets. 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.

Features

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

Key Benefits:

- **Increased Security –** Unprecedented insight into user behavior and changes taking place in your environment to identify both external and internal threats.
- **Simplified Audit & Compliance –** Proven method for tracking users and ensuring visibility into who is doing what in the environment with reports to back it up.
- **Empowered SIEM –** Feed SIEM single events representing a security threat instead of thousands of logs, singling out the needle and discarding the haystack all without relying on logs.
- **Real-time insight** into high severity activities

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 natively logging can provide.

Change Prevention – Add an additional layer of security and control to your Active Directory, Exchange, and Windows File System environments through integrated blocking capabilities at the finest levels.

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®, RSA® Security Analytics, and HP® ArcSight®. Events feed in real-time, formatted and parsed properly out of the box.

Dynamic Policies – Dynamically connect data from other sources to enrich the context of StealthINTERCEPT policies, such as a list of critical security groups to monitor for membership changes from your DLP solution or privileged accounts to monitor for unauthorized authentications from your PAM product.

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.

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

Benefits:

- **Preventative controls** increase security posture and reduce operational risk due to careless error
- **Full event details** adds context and reduces complexity associated with native log analysis
- **Proof of adherence** to compliance requirements for auditors
- **Reduced overhead** on critical systems due to elimination of reliance on native logs

About STEALTHbits Technologies

STEALTHbits is a data security software company. We help organizations ensure the right people have the right access to the right information. By giving our customers insight into who has access and ownership of their unstructured data, and protecting against malicious access, we reduce security risk, fulfill compliance requirements and decrease operations expense.

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