Data Sheet

StealthDEFEND®

Purpose-built User & Entity Behavior Analytics for Insider Threat Detection

Always a Step Behind

The findings of virtually any data breach report will depict the same story. Attackers are circumventing traditional security measures at the network perimeter and are after two things; credentials and data. However, even with clear-cut evidence of where to focus their efforts, organizations still struggle to keep up with attackers, incapable of separating the noise from the important events or distinguishing the normal from the abnormal.

StealthDEFEND is a purpose-built User & Entity Behavior Analytics (UEBA) solution designed to identify abnormal behavior indicative of account compromise. Laser-focused on the authentication and authorization hub of an organization's IT infrastructure – Active Directory – StealthDEFEND profiles users and systems using higher quality data than any native log can provide.

StealthDEFEND employs next generation machine learning technology that detects patterns not discernable through summary statistical analysis, and scalable architectural approaches that enable real-time detection of abnormal and nefarious activities – regardless of whether or not they originate from inside or outside your network.

Critical Capabilities

For years, organizations have leveraged statistical and rules-based analysis techniques to identify statistically significant deviations from the norm, accepting their susceptibility to false-positives, lack of context, and the necessity to pre-define the behavior to be identified. These approaches have also presented challenges associated with scale and the timeliness of alerts due to architectural limitations. Perhaps most importantly, however, is the quality of the data organizations have been forced to work with, and the quantity of data sources they've chosen to analyze, making an uphill battle even more difficult.

Features:

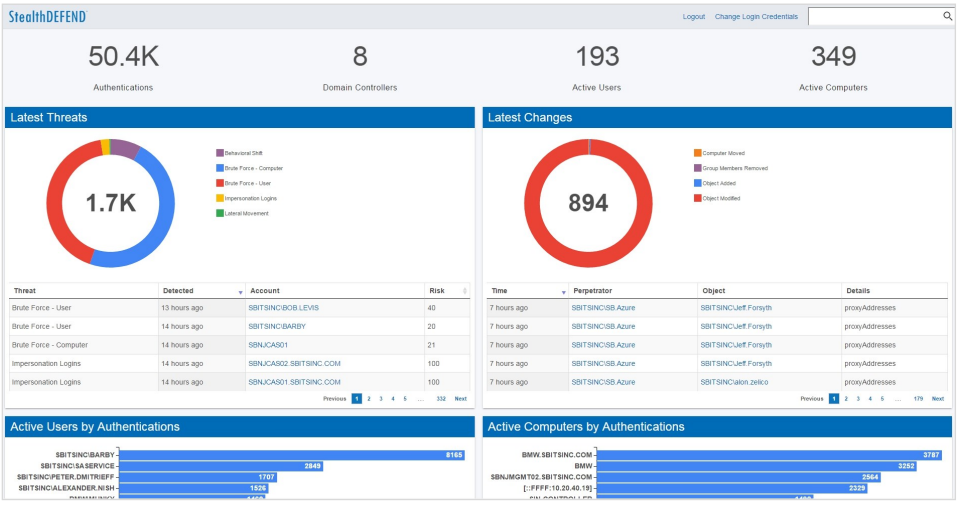
- **Behavioral Analysis** – StealthDEFEND automatically learns the behavior of each user and system, identifying outliers in real-time through approaches like Density-based Clustering and Time Series Analysis
- **Context Injection** – StealthDEFEND incorporates state-based information about users, systems, data access and sensitivity, and more to automatically risk-rate behavior for prioritized alerting and reporting
- **Threat Detection** – StealthDEFEND ships with predefined threat models aligning to common and sophisticated attack patterns
- **Damage Mitigation** – StealthDEFEND enables organizations to implement blocking of authentication and change activities associated with compromised accounts automatically or programmatically to stop attacks in their tracks

StealthDEFEND enables organizations to overcome these longstanding challenges through:

⇒ **The Right Focus**: Active Directory is under attack, and as the common thread between virtually everyone and everything across organizations large and small, it's the key target for attackers in almost every breach scenario. StealthDEFEND focuses on Active Directory because obtaining and leveraging credentials is fundamental to obtaining access to data, and Active Directory holds the keys to the kingdom.

⇒ **Better Data**: The data generated through native Active Directory logging is kluge, cumbersome, noisy, incomplete, and outdated. With its own instrumentation of Active Directory that bypasses native logging altogether, StealthDEFEND is able to consume a higher quality data set in real-time, void of noise and enriched with all the context and details needed to truly understand what users and systems are connecting to, from where, when, and how.

⇒ **The Right Architecture**: Statistical analysis relies on averages, purposely omitting the details that are so critical to detecting the outliers every organization is trying to identify. StealthDEFEND's usage of the latest advances in Machine Learning and Big Data technology not only allow it to monitor the millions upon millions of authentication events occurring on a daily basis, but maintain a complete history of the events and their details in a fashion available for real-time analysis.



StealthDEFEND's Index Page displays all activity from the past 24 hours in your environment, including latest threats detected, changes in Active Directory, active users and computers, and the total number of authentications.

- **Data Visualization** – StealthDEFEND surfaces threats through an easy to use and easy to understand HTML5 dashboard with drilldown and visualization of attacks
- **Real-Time Alerting** – StealthDEFEND will alert any audience of your choosing to identified threats in real-time
- **SIEM Integration** – StealthDEFEND can automatically send threats it's identified in real-time to a SIEM solution of your choosing for consolidated alerting

Benefits:

- **Plug-n-Play** – StealthDEFEND is delivered as a packaged, virtual appliance with no additional licensing costs
- **Real-Time** – StealthDEFEND detects attacks as they happen, in time for you to react and stop attacks before they become breaches
- **No Reliance on Native Logging** – StealthDEFEND efficiently monitors Active Directory authentications and changes without any reliance on native logging, providing more information at a fraction of the size

StealthDEFEND Threat Models

Category	Threat Models
Abnormal Behavior	Peer Group Deviation, Organizational Deviation
Behavior Shift	Baseline Deviation, First Time Access
Reconnaissance	Lateral Movement, Brute Force Attack, Honey Account, Stale Account Usage
Account Compromise	Concurrent Logons, Compromised Machine
Privilege Escalation	Golden Ticket, Administrative Access
Privileged Account Abuse	Service Account Misuse

Supported Platforms

Domain Controllers

- Windows Server 2008 or later
- 4GB+ RAM
- 50GB+ Disk Space available
- .NET 4.0 or later installed

StealthDEFEND Console

- VMWare or Hyper-V virtualization software
- 4 Virtual Nodes each having:
    - 32GB RAM
    - 4 Virtual Processors
    - 1TB Disk Space
    - A gigabit connection between all nodes in the cluster

About STEALTHbits Technologies

STEALTHbits Technologies is a data security 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
P: 1.201.447.9300 | F: 1.201.447.1818
sales@stealthbits.com | support@stealthbits.com
www.stealthbits.com