DATA SHEET

StealthDEFEND™ for File Systems

REAL-TIME THREAT ANALYTICS AND ALERTING

Corporate networks are under siege from attackers, requiring organizations to continually battle advanced threats like ransomware and attempts to exfiltrate or destroy their data. Securing unstructured data requires proactive interrogation of dozens of data points related to file access activity, including when, where, and how data is being accessed, who is accessing the data, and even each file's level of sensitivity. Until now, performing this level of analysis was either impossible or highly inaccurate and inefficient.

INTRODUCING StealthDEFEND

StealthDEFEND is the real-time threat analytics component of STEALTHbits' Data Access Governance Suite. Leveraging unsupervised Machine Learning, StealthDEFEND eliminates excessive and undifferentiated warnings to surface truly meaningful trends and alerts on attempts to compromise your sensitive data.

Purpose-Built

With over a decade of experience and expertise in the management and security of unstructured data to draw from, StealthDEFEND approaches real-time threat analytics and alerting for file system data through the mindset of an adversary.

Focused on file activity, important contextual elements like data sensitivity, and the actual attack methods leveraged in enterprise breaches, there is no better-aligned solution available to protect an organization's file system data against insider threats.

Cybersecurity Playbooks

The ability to detect and respond to threats quickly can mean the difference between a minor incident and a breach. Achieving this level of response speed is difficult for even the most seasoned security teams. StealthDEFEND simplifies threat response with the use of built-in Incident Response Playbooks that automate multi-stage actions ranging from basic alerting to triggering step-up authentication, greatly reducing insider threat dwell time.

Intelligent Indicators

As many organizations struggle to prioritize efforts among understaffed, overextended teams, the need for technology to lighten the load and the learning curve has never been more dire. StealthDEFEND comes prepackaged with advanced analytics and Machine Learning models that automatically evaluate and correlate the activity and behavior of the users interacting with your file system data. The result is a manageable quantity of incidences to investigate, supported by evidence that will justify the time spent.

Superior Data Quality

The data produced by native audit logging facilities is notoriously noisy, incomplete, and confusing. If input data is not complete, accurate, and timely, then the resulting output is subsequently unreliable and of little value.

StealthDEFEND is not only highly performant in its ability to collect and process millions of access events daily and in real-time, but eliminates reliance on native logging altogether, providing a consolidated, enriched stream of file activity data that produces the highest quality output.

Rapid Deployment

Time-to-value and overhead costs are major concerns for organizations of virtually any size. The longer a solution takes to deploy and the more resources it needs to perform properly, the lower its value becomes relative to other projects and priorities.

StealthDEFEND's modern architecture and design make it highly scalable and cost effective, requiring minimal infrastructure that can reside virtually anywhere, deploy in hours, and begin providing results immediately.

Increased ROI

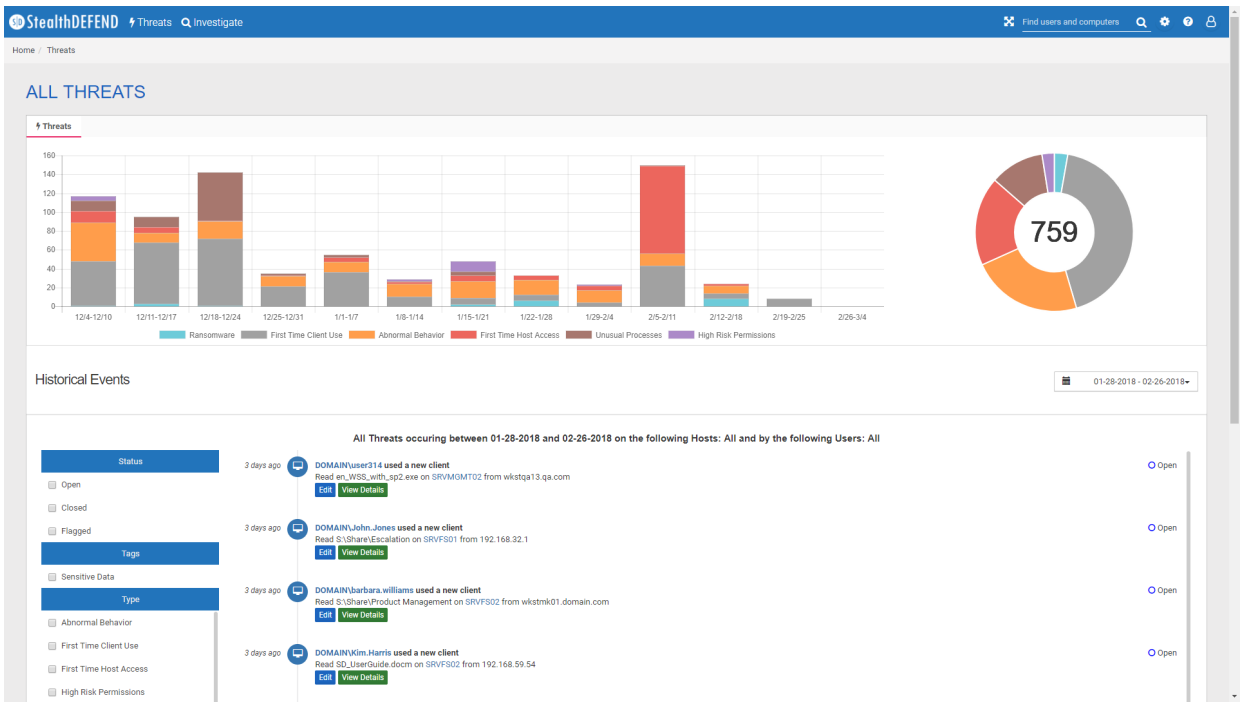
Products designed for interoperability enable organizations to automate manual processes, achieve efficiencies, and ultimately increase the ROI in the other investments they've made over time.

StealthDEFEND's RESTful APIs, certified integrations with market-leading SIEM vendors, and flexible exportation facilities enable users to maximize their investments in a wide variety of technologies, from DLP to Data Classification, SIEM, UBA platforms, and more.

TOP FEATURES

- Unsupervised Machine Learning – Analyze a rich set of data with Machine Learning models that evaluate, correlate, and baseline the activity and behavior of users.
- Seamless Sensitive Data Integration – Threat and data governance information is seamlessly integrated, further reducing noise by honing in specifically on the files that matter most.

- **Preconfigured Threat Models** - StealthDEFEND has been purpose-built to detect file system threats associated with Ransomware, Abnormal Behavior, First Time Host Access, First Time Client Use, Unusual Processes, and more.
- **User Behavioral Profiles** – Concrete understanding of each individual user's behavior is incorporated into StealthDEFEND's threat analytics and Machine Learning models, complemented by visuals that make understanding any user's normal behavior a trivial task.
- **Comprehensive Investigations** - Create, configure, and save detailed reports, alerts, and threats on User and Group activity.
- **SIEM Integration** – Out-of-the-box SIEM integration and preconfigured dashboards extend ready-to-use functions.
- **Real-Time Alerting** – Real-time security alerts powered by Machine Learning allow you to master your threat data in a continuous way that leads to faster investigations and threat neutralizations.
- **Interactive, Real-Time Visualizations** – Through a unified web presentation layer, threat data is streamed, processed, and visualized as it happens, including modern visualization elements like heat maps that update themselves in real-time to bring data to life.
- **Incident Detection Response Workflow** – Quickly coordinate your team's efforts so they're prepared to share information and track who is working on an issue at any given time.



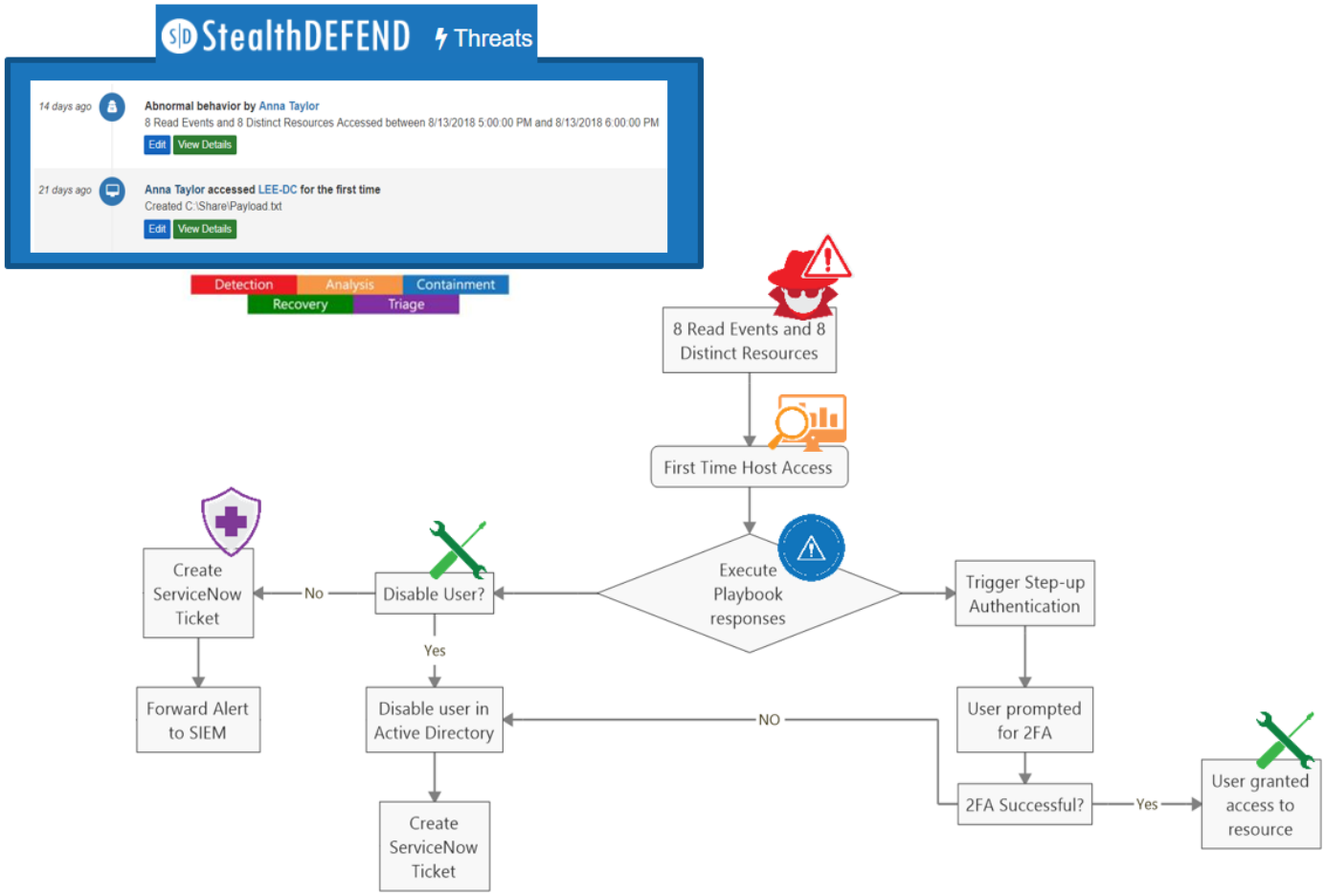
CYBERSECURITY PLAYBOOKS

The StealthDEFEND Actions Engine automates security responses and connects various security applications and processes together with multi-stage actions. This allows customers to build "Playbooks" they can use to respond to threats automatically or in an ad-hoc fashion.

The ability to detect and respond to threats quickly can mean the difference between a minor incident and a breach. Achieving this level of response speed is difficult for even the most seasoned security teams. StealthDEFEND's built-in Incident Response Playbooks can be used to automate multi-stage actions ranging from basic alerting to triggering step-up authentication, greatly reducing insider threat dwell time.

The following is one of the many Playbooks supported by StealthDEFEND and leverages the following response actions:

- *Step-Up Authentication*
- *User account disabling*
- *Incident Management Ticket creation*
- *SIEM Alert Generation*



DATA SHEET

TOP USE CASES

- Ransomware Behavior
- First-time Access
- Suspicious Encryption Activity
- Configuration File Tampering
- Abnormal User Behavior
- Unusual Process Execution
- Abnormal Denied Activity
- Mass File Deletions
- Unusual Sensitive Data Access
- Suspicious Permission Changes
- Data Exfiltration Attempts
- Lateral Movement

SUPPORTED PLATFORMS

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

DELL EMC:

- EMC Celerra 6.0+
- VNX:
  - VNX 7.1
  - VNX 8.1
- EMC VMAX3
- Isilon:
  - Isilon 7.0
  - Isilon 7.1
  - Isilon 7.2
- Unity

NETAPP:

- ONTAP 7.2+ (7-Mode and Cluster -Mode)

HITACHI:

- Hitachi 11.2+

STEALTHbits TECHNOLOGIES

STEALTHbits Technologies is a cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. DS-SDFS-0917