

# StealthDEFEND® FOR FILE SYSTEMS

Real-time detection and response for threats against file systems



**stealthbits**  
NOW PART OF **netwrix**

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 pro-active 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.

## WHAT IS StealthDEFEND FOR FILE SYSTEMS?

StealthDEFEND for File Systems is the real-time threat analytics component of Stealthbits' Data Access Governance Suite. Leveraging Unsupervised Machine Learning algorithms, advanced behavioral analysis, and important contextual elements such as data and account sensitivity, StealthDEFEND eliminates excessive and undifferentiated warnings to surface truly meaningful trends and alerts on attempts to compromise your sensitive data.

"Organizations are experiencing data loss across a wide range of content, formats, and methods—from documents to databases, stolen electronically or physically, and orchestrated by insiders or externals. More than 90% of security breaches in Asia-Pacific resulted in actual exfiltration of data, compared to 84% in North America and 80% in the UK."

*(Source: McAfee Report - Grand Theft Data)*

## KEY BENEFITS

### SIMPLIFIED FILE SYSTEM THREAT DETECTION

Advanced attacks against file data can be highly complicated, native audit logging is void of critical data needed to detect them. StealthDEFEND is designed to take the guesswork out of the equation.

### REDUCED TIME TO DETECTION

StealthDEFEND focuses on helping organizations reduce time to detection and containment resulting in lower cost should a breach occur.

### SUPERIOR DATA FIDELITY

Data produced by native audit logging facilities is notoriously noisy, incomplete, and confusing. StealthDEFEND provides a consolidated, enriched stream of file activity data that produces the highest quality output.

### INCREASED EFFICIENCY

Built-in integration with the market's leading SIEM solutions and other popular technologies such as ServiceNow, Slack, and Microsoft Teams ensures threat data resides in the places you need and want it most.

### INSTANT AWARENESS

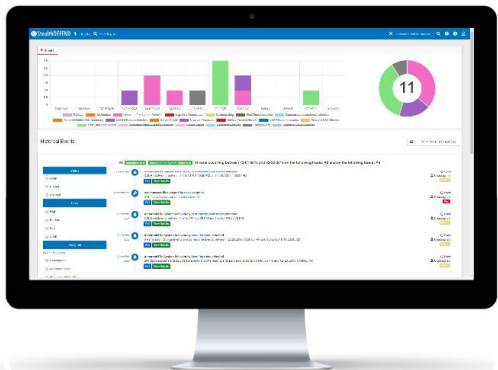
Truly real-time alerts are triggered instantly and can be delivered in a variety of ways, including email and integration with SIEM or other relevant technologies.

### ATTACK TIMELINE

StealthDEFEND makes it easy to visualize corresponding activities related to suspicious behavior through its attack timeline.

## ADVANCED ATTACKS, ABNORMAL BEHAVIOR AND SECURITY EVENTS

StealthDEFEND is purpose-built to detect and respond to both specific methodologies attackers are leveraging and the abnormal behaviors they exhibit when attempting to compromise file data.



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

## NEXT STEPS



**Schedule a Demo**  
[stealthbits.com/demo](https://stealthbits.com/demo)



**Download a Free Trial**  
[stealthbits.com/free-trial](https://stealthbits.com/free-trial)



**Contact Us**  
[info@stealthbits.com](mailto:info@stealthbits.com)

## KEY FEATURES

### AUTO-RESPONSE PLAYBOOKS

StealthDEFEND provides an extensive catalog of preconfigured response actions that automatically respond when threats are identified. These playbooks can be easily shared across your organization to standardize threat responses.

### BEHAVIOR ANALYTICS

Identify outlier activity compared to 'normal' behavior. We can analyze large amounts of events and elevate uncommon or suspicious behaviors to be immediately reviewed.

### SEAMLESS SENSITIVE DATA INTEGRATION

Threat and data governance information is seamlessly integrated through StealthAUDIT and other 3rd Party products (e.g. DLP solutions), further reducing noise by honing in specifically on the files that matter most.

### COMPREHENSIVE INVESTIGATIONS

An attack is frequently a collection of related activities that tell a larger story. StealthDEFEND pulls together all related events to simplify the compiling of digital case files.

### USER-DEFINED THREATS

Define threats and their parameters in alignment with your organization's specific needs and requirements. Reduce false positives with revised rules, logic, and criteria dedicated to handling exclusions with ease.

### DECEPTION TOOLS

Proactively lure attackers into making the wrong move with built-in Honeypot token deployment, management, and detection capabilities that are easy to administer and simple to deploy.

## 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.

©2020 Stealthbits Technologies, Inc.