stealthDEFEND

StealthDEFEND® FOR FILE SYSTEMS

Real-time detection and response for threats against file systems

stealthbits

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, which is why StealthDEFEND is designed to take the guesswork out of the equation.

ENHANCED AND REDUCED TIME TO DETECTION

StealthDEFEND focuses on helping organizations reduce time to detect and contain breaches.

SUPERIOR DATA FIDELITY

The data produced by native audit logging facilities is notoriously noisy, resource intensive, incomplete, and confusing. StealthDEFEND is not only highly performant, but eliminates the challenges presented by native logging altogether, providing a consolidated, enriched stream of file activity data that produces the highest quality output.

INCREASED EFFCIENCY

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

RESPONSE PLAYBOOKS

StealthDEFEND provides automated response options when threats are identified. These playbooks can be easily shared across your organization to standardize threat responses. In addition to an extensive catalog of preconfigured response actions, StealthDEFEND can integrate with your own business processes using PowerShell or webhook facilities.

MACHINE LEARNING & USER BEHAVIOR ANALYTICS (UBA)

Identifies outlier activity as compared to the behavior profile created by the unsupervised learning engine. This allows a large amount of events to be analyzed and suspicious behaviors to be elevated for review automatically.

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 allow administrators to perform comprehensive investigations for forensic compilation of digital case files.

USER-DEFINED THREATS

StealthDEFEND allows administrators to easily add new threats that align to their organization's specific requirements. To reduce false positives, administrators can add thresholds for how many times an activity can occur before action is taken.

NEXT STEPS

Schedule a Demo

stealthbits.com/demo

Download a Free Trial

stealthbits.com/free-trial

Contact Us

info@stealthbits.com

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.