SOLUTIONS SHEET

DIGITALGUARDIAN®
User Activity Monitoring

USER ACTIVITY MONITORING FOR FEDERAL AGENCIES

Traditional federal security solutions tend to focus on infrastructure, but overlook the employee or contractor. This can create a blind spot for your agency, preventing you from knowing what data users are accessing and what they're doing with it. This security void, combined with increasingly open networks among agencies, contractors and programs, leaves your sensitive data vulnerable.

MANY GOVERNMENT WORKERS DON'T CONSIDER SECURITY WHEN SHARING WITH THIRD PARTIES

31% WSJ

of government workers said they never or only occasionally consider data security or privacy issues into account when they share information with vendors or other external stakeholders.

(Source - Wall Street Journal, Survey: Many Government Employees Use Personal Email for Work, Sep 1, 2015)

VISIBILITY TO INSTANTLY DETECT SUSPICIOUS USER BEHAVIOR

Digital Guardian User Activity Monitoring offers complete user visibility and control regardless of what users are running, what they're running it on, and whether or not they're on the network. Your agency can audit, monitor, limit and report on all end-user activity in real-time, and also perform investigative tasks. Our solution helps government pros classify, categorize and tag data so every action is tracked and accounted for – providing a detailed audit trail that can aid investigations and help your agency show compliance with mandates like Insider Threat Executive Order 13587.

Whether it's deployed on premise or as a cloud-based managed service, Digital Guardian begins to work as soon as it's installed, enabling instant detection, investigation and containment of suspicious activity.

> "Implementation is greatly simplified… with average deployment times much shorter than other DLP products. It can often be completed in a single day, with only minimal policy tuning required thereafter."

DLPX DATA LOSS PREVENTION EXPERTS

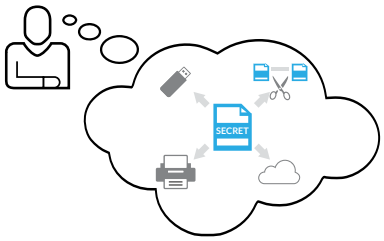
(Source - Data Loss Prevention Leading Vendors Review, DLP Experts, 2016)

SMALL BUSINESS CERTIFIED

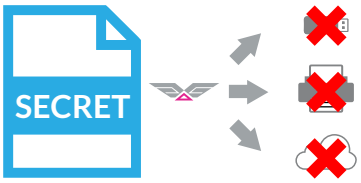
DIGITALGUARDIAN®

For more information, visit
www.digitalguardian.com

USER ACTIVITY MONITORING IN ACTION



Agency does not know if, when, or how users mishandle sensitive data



Digital Guardian confirms some users attempting to violate agency's acceptable use policies

Digital Guardian enforces role-based policies to control how data is handled & egressed

Digital Guardian educates & shapes user behavior in real time to ensure policy compliance

KEY BENEFITS

CONTINUOUSLY RECORD EVERY USER ACTION WITH SENSITIVE DATA

- Track every system, data, application, and network event for each user
- Detect abnormal file operations or unauthorized attempts to exfiltrate
- Establish malicious intent by analyzing suspect actions in complete context
- Capture files, screen shots and keystroke logging before and after suspicious activity

IDENTIFY SUSPICIOUS USER BEHAVIORS THAT DEVIATE FROM NORMAL DATA USE

- Establish user trends to baseline normal behavior and block/prompt/alert extreme exceptions
- Identify suspicious/unauthorized applications used to access data
- Detect suspicious system configuration changes; alert when users deviate from normal activity

MONITOR, RECORD AND CONTROL TRUSTED USERS HANDLING SENSITIVE DATA

- Identify privileged users and control their use of sensitive data
- Prevent nonessential file access and operations by administrators
- Detect and investigate anomalous user behavior
- Prevent tampering with or circumventing policy controls

INVESTIGATE SUSPICIOUS BEHAVIOR AND PROVE MALICIOUS INTENT

- Collect and preserve chain-of-custody forensic evidence including capture files, screenshots and keystrokes
- Reconstruct incidents in their full context

MANAGE EVIDENCE FOR ACTIVE INVESTIGATIONS WITH ROLE-BASED CONTROLS

- Store evidence within a secured repository in the management console
- Collect and preserve forensics from target systems without physically securing the device
- Allow investigators to analyze evidence with elevated privileges

ABOUT DIGITAL GUARDIAN FEDERAL

Digital Guardian helps government respond with certainty and effectiveness at the speed and scale of threats. Our threat-aware data protection software focuses on defending every moment in the life of government data – no matter how it's structured, where it lives or how it's used. Our data-centric platform for data integrity, insider and outsider threat protection, and user activity monitoring is an ideal match for today's boundary-less networks that span agencies, contractors and programs. Your agency can maintain mission integrity while protecting America's most vital information assets.

Public Sector Headquarters
12020 Sunrise Valley Dr.,
Suite 350
Reston, VA 20191
Phone 703-956-2358

Copyright © 2016 Digital Guardian, Inc. All rights reserved. Digital Guardian and Security's Change Agent are trademarks of Digital Guardian, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.

SHARE