With the rising value and volume of digital assets within agencies, there’s greater risk of insiders stealing sensitive data. Once you grant insider access to your network, perimeter security offers no defense. Bad actors enjoy the latitude that comes with trusted access, and can easily compromise data without detection. That’s why guarding against insider threats requires a focus on securing the data itself.

The primary security threat facing federal organizations is the negligent insider.


A 2016 Gartner survey found that only 18% of organizations have a formal program in place to address the insider threat. Digital Guardian provides data-centric security via enterprise wide visibility, real time user education, and flexible deployment options all designed to stop insider threats.

Digital Guardian offers one of the most advanced and powerful endpoint DLP agents due to its kernel-level OS integration. In addition to Windows, both Apple OS X and Linux are supported.

...Digital Guardian [is one of] two vendors most frequently mentioned by clients looking for a managed services option.

Digital Guardian DLP is a consistent leader in the Gartner Magic Quadrant for Enterprise DLP with support for Windows, OS X and Linux. It proactively tags and classifies data as soon as you install it, offering immediate protection from the start – allowing your agency to stay ahead of threats before they happen.

A DATA-CENTRIC APPROACH TO INSIDER THREAT PROTECTION

A 2016 Gartner survey found that only 18% of organizations have a formal program in place to address the insider threat. Digital Guardian provides data-centric security via enterprise wide visibility, real time user education, and flexible deployment options all designed to stop insider threats.

THE BROADEST VISIBILITY AND CONTROL AGAINST INSIDER THREATS

Digital Guardian’s insider threat solution offers the deepest visibility, fine-grained control and the industry’s broadest DLP coverage – ensuring that whether you face malicious or inadvertent actors, your agency’s confidential data never leaves your organization.

With advanced methods for detection, access control, activity monitoring and analysis, Digital Guardian supports compliance with key mandates related to insider threats, including NISPOM2 and Executive Order 13587.

Digital Guardian DLP is a consistent leader in the Gartner Magic Quadrant for Enterprise DLP with support for Windows, OS X and Linux. It proactively tags and classifies data as soon as you install it, offering immediate protection from the start – allowing your agency to stay ahead of threats before they happen.

Digital Guardian offers one of the most advanced and powerful endpoint DLP agents due to its kernel-level OS integration. In addition to Windows, both Apple OS X and Linux are supported.

...Digital Guardian [is one of] two vendors most frequently mentioned by clients looking for a managed services option.

(Sources: Gartner Magic Quadrant for Enterprise Data Loss Prevention, 1 February, 2016, Brian Reed and Neil Wynne. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designations. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.)
Most DLP products require you to create complicated, approved policies first. But with Digital Guardian DLP and automated data classification, you can get instant insight into where sensitive data is located, how it flows in the organization, where it is put at risk.

**INSIGHT**
Get instant insight into how sensitive data is used.

**BUILD**
Create policies based on data usage.

**EDUCATE**
Create awareness in real-time on how to safely handle sensitive data.

**ACT**
Configure rules to enforce user actions.

**ASSESS**
Provide a mechanism to continuously assess, iterate and improve security policies and procedures.

### KEY BENEFITS

**PREVENT UNAUTHORIZED EXFILTRATION OF DATA VIA WEB, EMAIL, SOCIAL MEDIA SITES OR MEDIA STORAGE**
- Ensure sensitive data is encrypted when exfiltrated from the corporate domain
- Block file uploads to personal webmail or social media accounts
- Require user justifications for policy exceptions
- Maintain exfiltration policies if users encrypt or suspiciously alter data

**BLOCK DATA EXFILTRATION TO UNAUTHORIZED CLOUD STORAGE**
Disallow sensitive files copied to personal Dropbox, Box.net, etc. accounts (but allow the ability to access if a corporate version)
- Block downloads of sensitive data in corporate cloud storage to BYOD devices (but allow to be viewed on the device)
- Ensure sensitive data is encrypted before uploaded to cloud storage

**IDENTIFY SUSPICIOUS 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

**PERSISTENTLY MONITOR AND CONTROL SENSITIVE DATA FOR PRIVILEGED USERS**
- Enforce role-based access controls to sensitive files
- Block authorized actions if risky/suspicious (e.g., allow printing of IP on the corporate network, but block if printing at home.)

**GAIN REAL-TIME USER EDUCATION/AWARENESS OF NONCOMPLIANCE AND BLOCK MALICIOUS BEHAVIOR**
- Enforce secure business processes that make users aware and accountable to data risks
- Measure rates of noncompliant activity before and after training/warning prompts are enabled
- Confirm users haven’t taken sensitive data prior to leaving the company (e.g., exit interview use case)

**KEEP SENSITIVE DATA IDENTIFIABLE IF OBSCURED TO AVOID DETECTION**
- Ensure policies are accurately enforced for sensitive data throughout its lifecycle
- Monitor potentially risky file operations (e.g., save as, delete, cut and paste)
- Block or alert when sensitive data is zip-encrypted or screen captured
- Ensure files with content copied from another sensitive file are classified the same as the original

© 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.