Public-sector security pros must be ready to sense, locate and stop threats of any size at any time, across every kind of data. But more of these threats are coming from unfamiliar vectors and unexpected actors – including employees and contractor insiders.

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. This 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 with our:
• Unique data awareness capabilities
• Transformative endpoint visibility
• Behavioral threat detection and response

Whether deployed on premise or through our Managed Security Program, Digital Guardian solutions integrate with the security platforms public agencies already use – helping you manage your data protection through a single pane of glass.

Our portfolio is easy to acquire and deploy. We’re a GSA Schedule 70 contract holder with access to multiple other contracts through our channel partners. Meanwhile, our cost-effective solutions, licensing plans and delivery options help maximize lifecycle value across your agency’s cyber investments and programs.

INCIDENT REPORTS RECEIVED BY US CERT

57,971 FY2013
75,087 FY2015

(source - Annual Report to Congress: FISMA, OMB, March 18, 2016)
DATA INTEGRITY

Achieve Compliance Faster and with Greater Confidence

Almost all federal agencies are impacted by compliance mandates designed to protect the integrity of critical government records against accidental and malicious threats.

To achieve compliance with these mandates, agencies must be able to identify critical data throughout their organization, classify it, and put controls in place to protect this data from being altered, lost or stolen.

Digital Guardian provides the industry’s most accurate technology for identifying and controlling sensitive data including ePHI and PII. Our solution is the easiest to implement and manage, and delivers the lowest false-positive rates. And with our advanced visibility, monitoring and reporting, your agency can more easily achieve and demonstrate compliance with HIPAA, PCI DSS, NIST SP 800-53, NIST SP 800-137 and NIST SP 800-171.

The Digital Guardian for Compliance suite includes tools that support data discovery, monitoring, control and security throughout your entire IT environment – on networks, network servers, end-user devices, or in the cloud. You can deploy the platform on premises with low total cost of ownership, or as a managed service via our Managed Security Program.

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.

USER ACTIVITY MONITORING

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.
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.

Together, these provide your agency with the highest level of protection from an array of threats, including polymorphic malware, zero-day attacks, advanced persistent threats (APTs), ransomware, and attacks using other sophisticated data theft methods.

The Digital Guardian solution for endpoint covers DLP and endpoint detection and response (EDR) in a single agent form factor installed on desktops, laptops and servers running Windows, Linux or Apple OS X, as well as support for virtual desktop infrastructure (VDI) environments.