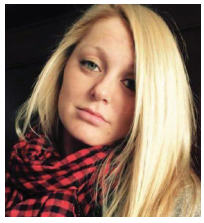
Group Test: DLP

Digital Guardian
Rated 5/5 Stars & the Best Buy

Data loss prevention



Securing data has become a labor-intensive task due to tremendous increases in volume and the far-reaching vectors it traverses. Only recently have compliance standards and frameworks cracked down on information security practices and most organizations still do not sufficiently monitor their data or control its accessibility. The aggressive changes in security protocols and tightened compliance standards affirm the importance of data loss prevention solutions, which control access and monitor behavior to prevent the improper handling or transfer of data.

Including tools like machine-learning-based behavior analysis and relationship graphs to advanced monitoring techniques, these products narrow the gap between actual and adequate data security practices. Unlike other product groups, the data loss prevention group does not necessarily appeal to a specific industry or organization. All organizations, regardless of size, need to incorporate data loss prevention into their security posture, and we are confident that at least one of these tools will suit most business needs. Some organizations may even choose to deploy more than one option for bolstered data security.

For security professionals that value their data (that should be all of you), we strongly endorse these products and recommend integrating them into your environments. All organizations should now consider data loss prevention tools to be security staples since their importance will only increase in the foreseeable future.

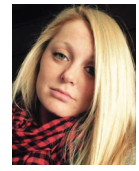
– Katelyn Dunn

Products review team

Rob Cote, program director

Dan Cure, technical writer

Michael Diehl, technology editor



Katelyn Dunn, technical writer

Matthew Hreben, security technologist

Judy Traub, interim program project manager

Tom Weil, security analyst

Steve Zurier, program project manager

How we test and score the products

Our testing team includes SC Lab staff, as well as external experts who are respected industry-wide. In our Group Tests, we look at several products around a common theme based on a predetermined set of SC Lab standards (Performance, Ease of use, Features, Documentation, Support, and Value for money). There are roughly 50 individual criteria in the general test process. These criteria were developed by the lab in cooperation with the Center for Regional and National Security at Eastern Michigan University.

We developed the second set of standards specifically for the group under testing and used the Common Criteria (ISO 1548) as a basis for the test plan. Group Test reviews focus on operational characteristics and are considered at evaluation assurance level (EAL) 1 (functionally tested) or, in some cases, EAL 2 (structurally tested) in Common Criteria-speak.

Our final conclusions and ratings are subject to the judgment and interpretation of the tester and are validated by the technology editor.

All reviews are vetted for consistency, correctness and completeness by the technology editor prior to being submitted for publication. Prices quoted are in American dollars.

What the stars mean

Our star ratings, which may include fractions, indicate how well the product has performed against our test criteria.

★★★★★ Outstanding. An "A" on the product's report card.

★★★★ Carries out all basic functions very well. A "B" on the product's report card.

★★★ Carries out all basic functions to a satisfactory level. A "C" on the product's report card.

★★ Fails to complete certain basic functions. A "D" on the product's report card.

★ Seriously deficient. An "F" on the product's report card.

SC MEDIA LAB APPROVED | SC MEDIA BEST BUY | SC MEDIA RECOMMENDED

What the recognition means

Best Buy goes to products the SC Lab rates as outstanding.

Recommended means the product has shone in a specific area.

Lab Approved is awarded to extraordinary standouts that fit into the SC Lab environment, and which will be used subsequently in our test bench for the coming year.

Data loss prevention

Data loss prevention products also come with automation capabilities that minimize the laborious nature of data security, increase response time and reduce human error, says Katelyn Dunn.

PICK OF THE LITTER

Digital Guardian Data Protection Platform focuses on content, context and user-based classifications to appropriately tag and fingerprint sensitive data without adding more false positive results. This highly content- and context-aware solution provides substantial visibility, control, protection and compliance support in a single package. This solution is both comprehensive and competitively priced, making it an SC Labs Best Buy.

Zecurion DLP covers our list of features and tops it off with more than ten different content detection technologies, giving it extensive monitoring capabilities. Its robustness combined with its unparalleled monitoring and access control make Zecurion our SC Labs Recommended product for this month's round of reviews.

This month, the SC Labs team looked at the data loss prevention space, where products control access and monitor behavior to ensure that end-users do not improperly transfer company information or files. The value of sensitive data has recently encouraged organizations to invest more resources in data loss prevention and these investments have, in turn, directly reduced organizational risk and compromise events.

At this point, most organizations operate predominately – even exclusively – with electronic data. Companies either duplicate their paper files electronically or convert them to electronic format and then archive them. Therefore, the amount of data security teams and administrators must protect and the vectors they must secure has grown exponentially in businesses great and small, and organizations have often not done nearly enough on the security front to adjust to this increase.

The discrepancy between adequate data security and actual data security has spawned information security compromises, some of which resulted in unmitigated technological disasters and public relations nightmares. Some of those organizations have suffered severe financial consequences and the loss of customer trust, necessitating a change in information security practices as well as new and tightened compliance standards.

The sheer number of data points makes tracking and monitoring files and corporate content extremely difficult, further complicating the practice of data loss prevention. Trying to adequately configure data protection while not hindering productivity can be a challenging task to navigate. From a security standpoint, there is an inherent drive to make a security posture as airtight and impenetrable as possible. However, doing so interferes with streamlined processes and may even inhibit employee efficiency when it comes to task completion.

This interference arises because of the stringent policies and settings that airtight security mandates. Employees may be unable to access certain files or applications without requesting access to them first.

This additional step dramatically increases the overall time required to complete tasks, which, in turn, reduces production. We saw many impressive features in this space geared toward airtight access control, anomalous behavior detection and information monitoring.

As in other areas of cybersecurity, data loss prevention products also come with automation capabilities that minimize the laborious nature of data security, increase response time and reduce human error.

From standard security features to more advanced monitoring techniques like keystroke capture and end-user behavioral analysis, these six products impressed us with their innovative developments.

Data loss prevention solutions, such as the ones featured here, are vital in the fight to protect valuable data and limit data vulnerabilities. In some cases, organizations may prefer to deploy more than one of these data loss prevention products to reach an optimal security posture.

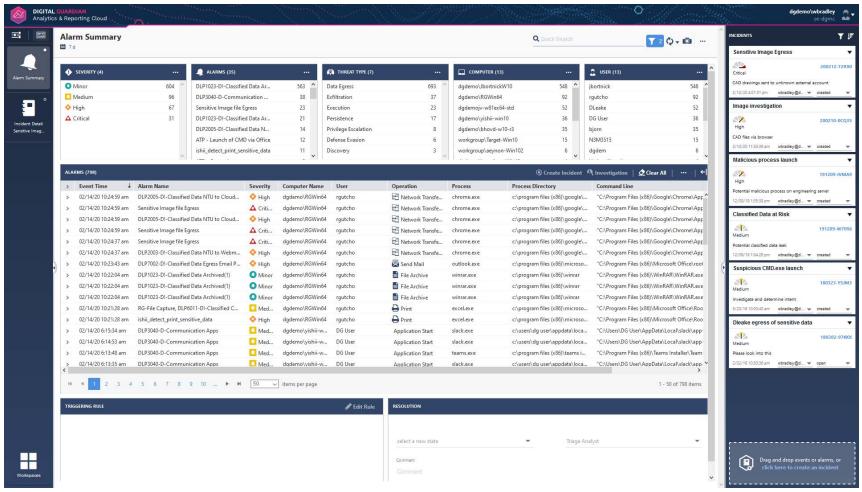
The vendors have not customized these products for any specific industry or type of organization. Everyone needs to incorporate data loss prevention into their security practices and should consider these products a staple in any security toolset.

Specifications for data loss prevention

●=yes =no

Product	Code 42	Digital Guardian	Fidelis Security	iStorage	McAfee	Zecurion
Analytics and reporting	●	●	●	●	●	●
Management console	●	●	●	●	●	●
Data discovery	●	●			●	●
Data classification		●			●	●
Endpoint DLP	●	●			●	●
Network DLP		●	●		●	●
Cloud data protection	●	●	●	●	●	●
Event management workflow	●	●	●		●	●
Managed services		●	●	●	●	●
Network appliance		●	●		●	

Digital Guardian
Data Protection Platform 7.6



DETAILS

Vendor Digital Guardian

Price $15 - $25 per seat, per year

Contact digitalguardian.com

Features	★★★★¾
Documentation	★★★★★
Value for money	★★★★★
Performance	★★★★★
Support	★★★★★
Ease of use	★★★★★

OVERALL RATING ★★★★★

Strengths The visibility provided by comprehensive data discovery and thorough content-based classification.

Weaknesses None that we found.

Verdict Focused on content, context and user-based classifications resulting in powerful information used to identify, tag, and fingerprint sensitive data with the lowest possible false possible results.

Digital Guardian Data Protection Platform offers data protection independent of threat actors, data types, systems, applications, devices or points of access. This cloud-based model unifies endpoint detection, response and data loss prevention to protect against internal threats and accidental data loss or purposeful theft, using the same agent.

BEST BUY

Endpoint detection and response protect against outsider threats and attackers masquerading with stolen credentials, preventing them from accessing or manipulating data. Digital Guardian offers three managed security programs: endpoint DLP, managed detection and response and network DLP.

The entirety of this platform focuses on content, context and user-based classifications. Content-based analysis inspects files to identify, tag and fingerprint sensitive data for the lowest possible false positive results. It also identifies and tags structured and unstructured sensitive data to give visibility into the data source. User-based classification lets users classify sensitive data based on organization-specific business requirements.

Extensive data, user and system events are monitored and recorded for prompt and efficient detection of anomalous behaviors, data manipulation and system modifications. These events are displayed in the new and fully customizable elastic dashboard, the Analyst Reporting Console (ARC). ARC is intuitive, with easy-to-follow drilldown capabilities and filters. All collected data is aggregated in ARC and can be exported as reports that reveal when and how classified data has egressed.

Alarms run based upon server-side rules and support graphically based investigations for better visibility and response times. This approach uncovers powerful information that shows what end-users are doing with data so that administrators and investigative teams can spot and contain policy violations. These investigations can also be used to leverage trend information for policy and rule creation. Alerts can even be issued to the individuals responsible for an unwanted event.

Digital Guardian Data Protection Platform sports many impressive features, including automated adaptive classification and comprehensive visibility. This highly content- and context-aware solution offers everywhere-all-the-time data protection using one, multi-function agent for minimal operational overhead. It is a worthy contender in the DLP space and ideal for anyone looking for data visibility and control, an investigation module, insider/external threat protection and compliance support in a single package.

Pricing starts at a range of $15-$25 per seat, per year and includes 24/7 phone, email and website support.

— Katelyn Dunn
Tested by Tom Weil