DATASHEET

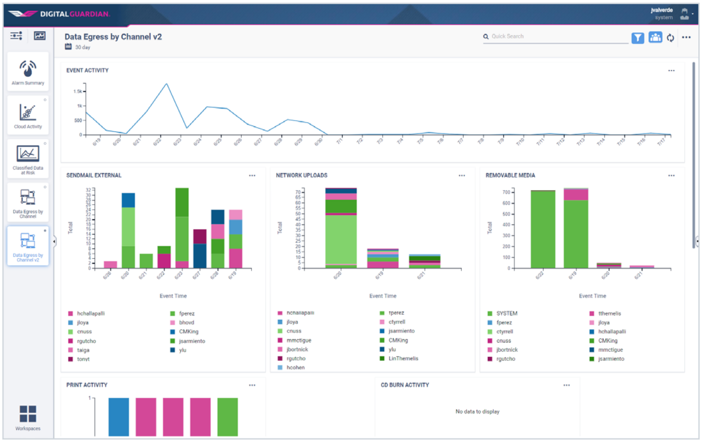
DIGITALGUARDIAN®

# Digital Guardian Endpoint Data Loss Prevention

## Protect Sensitive Data on ALL Your Endpoints

Digital Guardian Endpoint Data Loss Prevention (DLP) gives you everything you need – the deepest visibility, the fine-grained control and the industry's broadest data loss protection coverage – to stop sensitive data from getting out of your organization at the greatest point of risk – the endpoint.

Our proven, endpoint agent captures and records all system, user and data events on or off the network. You can configure the agent to automatically block suspicious insider activity or outsider attacks – malware and malware-free - before sensitive data is lost.



## Deepest and Broadest Visibility

### Deepest and Broadest Visibility

Our solution offers the industry's broadest protection coverage recognizing both structured and unstructured files running on multiple systems both on and off the network. With Digital Guardian, you have complete data visibility and control regardless of what users are running, what they're running it on, and whether or not they're on the network.

### Full Platform Coverage

Sensitive data doesn't just exist on Windows machines. Only Digital Guardian delivers full data protection capabilities on Windows, Linux, and Mac machines to protect your data regardless of where it is created or used.

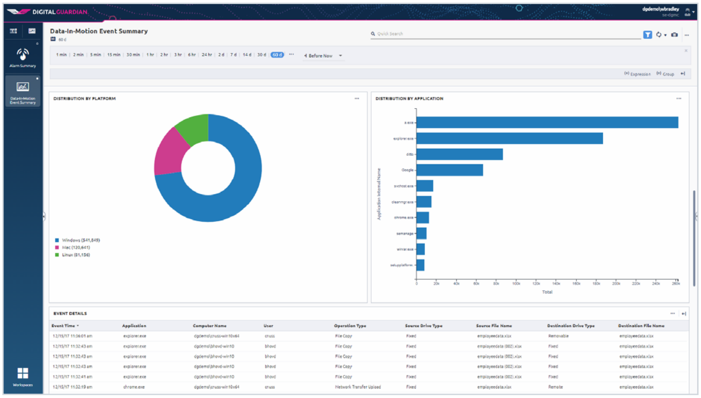
### Automated Classification

Most data loss prevention solutions require you to spend weeks or months identifying and classifying your sensitive data before protection starts. Digital Guardian begins as soon as you install it, proactively tagging and classifying both intellectual property and regulated information such as PII, PCI and PHI data.

# Key Benefits

## Intellectual Property and Personal Information

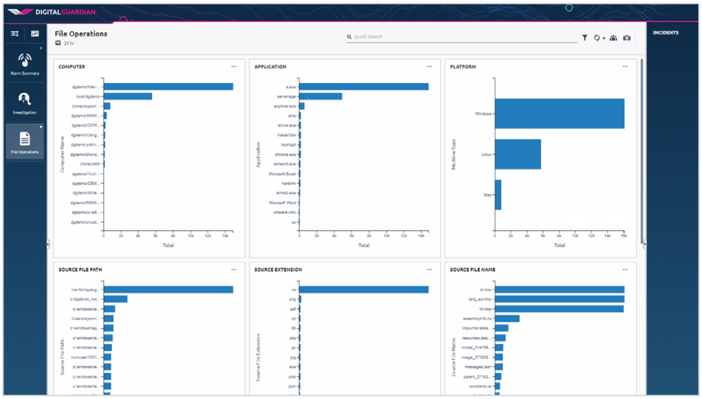
Digital Guardian Endpoint DLP finds, understands, and protects all data types including structured data such as PII and unstructured data such as intellectual property. Our comprehensive context and content awareness sees events at the system, user, and data level. This broad perspective enables more effective visibility and DLP controls for all of your organization's sensitive data.



| Event Time | Application | Computer Name | User | Operation Type | Source Drive Type | Source File Name | Destination Drive Type | Destination File Name |
|---|---|---|---|---|---|---|---|---|
| 12/15/17 11:36:01 am | explorer.exe | dgdemo\cruss-win10x64 | cruss | File Copy | Fixed | employeedata.xlsx | Removable | employeedata.xlsx |
| 12/15/17 11:32:43 am | explorer.exe | dgdemo\bhovd-win10 | bhovd | File Copy | Fixed | employeedata (002).xlsx | Fixed | employeedata.xlsx |
| 12/15/17 11:32:43 am | explorer.exe | dgdemo\bhovd-win10 | bhovd | File Copy | Fixed | employeedata (002).xlsx | Fixed | employeedata.xlsx |
| 12/15/17 11:32:43 am | explorer.exe | dgdemo\bhovd-win10 | bhovd | File Copy | Fixed | employeedata (002).xlsx | Fixed | employeedata.xlsx |
| 12/15/17 11:32:41 am | explorer.exe | dgdemo\bhovd-win10 | bhovd | File Copy | Fixed | employeedata (002).xlsx | Fixed | employeedata.xlsx |
| 12/15/17 11:32:19 am | chrome.exe | dgdemo\cruss-win10x64 | cruss | Network Transfer Upload | Fixed | employeedata.xlsx | Remote | employeedata.xlsx |

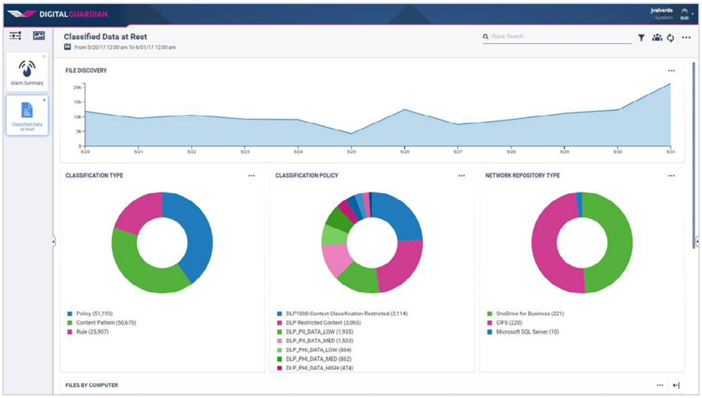
## Granular Control of All Data Movement

Automatically log, block, require justification, or encrypt sensitive data in or attached to email, files moved to removable drives, cloud storage, or web. Assign access permissions and encryption methods to removable devices or media. Limit the types of files which can be transferred onto removable devices / media, and the amount of data which may be transferred by time interval (e.g., MB per day). Restrict data movement to devices/media by brand, model or serial number.



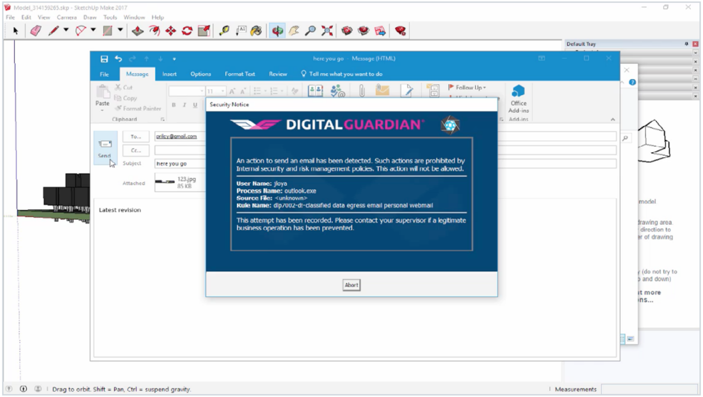
## Built-in Advanced Data Classification

Create and modify classification and usage policies through content inspection, context-awareness and user classification. Granular classification enables you to prioritize data protection efforts on the most sensitive data.



## DLP Only When You Need It

Design policies with controls that won't block actions that comply with corporate policy so employees remain productive while the data stays safe. Our DLP software automatically blocks only those actions that pose a threat to your organization. Its unique, contextual awareness lets you minimize risk while maintaining the pace of your business.



An action to send an email has been detected. Such actions are prohibited by Internal security and risk management policies. This action will not be allowed.

**User Name:** jloya
**Process Name:** outlook.exe
**Source File:** <unknown>
**Rule Name:** dlp7002-dl-classified data egress email personal webmail

This attempt has been recorded. Please contact your supervisor if a legitimate business operation has been prevented.

## ABOUT DIGITAL GUARDIAN

Digital Guardian's threat aware data protection platform safeguards your sensitive data from the risks posed by insider and outsider threats.

By harnessing our deep data visibility, real-time analytics and flexible controls, you can stop malicious data theft and inadvertent data loss.

DIGITALGUARDIAN®

SHARE