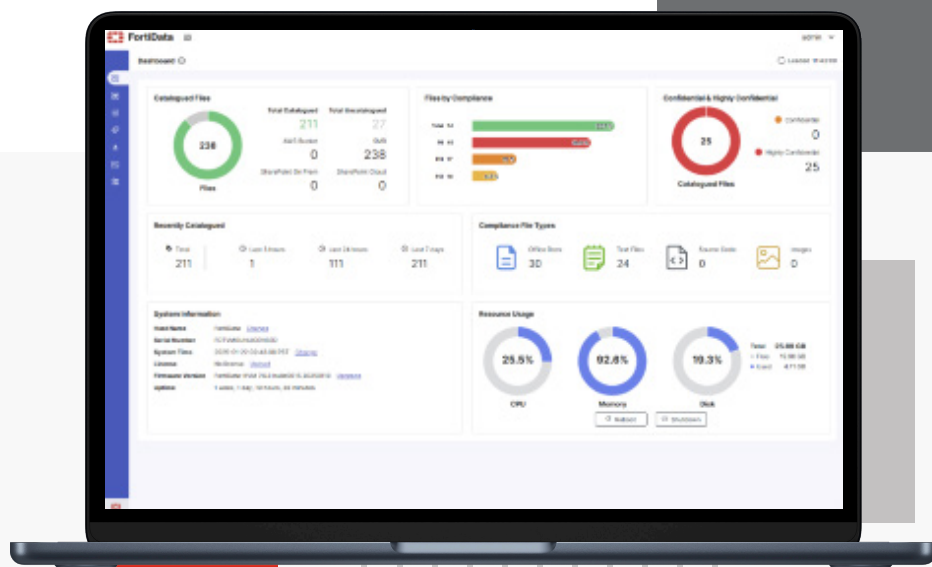


# FortiData

AI-Powered Data Discovery and Classification



## Key Use Cases

- Discovers sensitive data at rest across hybrid environments
- Classifies and labels sensitive data based on predefined and customizable data types
- Centralizes and dynamically visualizes your organization's current data security posture
- Helps organizations comply with data protection requirements associated with major compliance frameworks
- Identifies sensitive data present in image files through OCR

## FortiData for Data Security Posture Management

Today's most valuable currency is data. Whether it's PII, PHI, customer cardholder information, intellectual property, strategic plans, or financial account details, data is the lifeblood of digital organizations. It must always be protected from theft or exposure by threat actors, malicious insiders, and careless or untrained employees.

AI-powered FortiData works to bring together the full force of Fortinet's data protection capabilities across the Fortinet Security Fabric to provide security teams with a complete view of their data security posture when it comes to protecting sensitive data in use, in motion, and at rest across their organizations. FortiData also complements other Fortinet solutions by discovering, classifying, and labeling to enhance data loss prevention.

## Challenges: Increasing Complexity in Managing and Protecting Sensitive Data

Security and IT teams are faced with a two-fold challenge—their organizations are generating and collecting data at a rapid pace while the hybrid nature of today's networks means that data sprawl is an acute problem. Meanwhile, the use of multiple security products and fragmented data security coverage, with policies separately configured and managed, exacerbate the challenge.

FortiData works to simplify data protection by discovering, classifying, and labeling sensitive data, enhancing data loss prevention across a customer's use of the Fortinet Security Fabric, and providing centralized visibility into sprawl of sensitive data across an organization's on-premises and cloud data stores.

## Our Approach

FortiData is intended to unify data protection under a single dashboard to address the challenges associated with securing data in today's complex hybrid environments.

FortiData brings together powerful, automated data discovery, classification and labeling.

FortiData has one of the largest libraries of 400+ predefined data identifies and 200+ data templates.



### Centralized Data Visibility

For most Security and IT teams, visibility into data is fractured across multiple data stores and locations. FortiData is designed to discover and classify data across those disparate data stores to create a centralized view of sensitive data. Administrators can configure their own scans, reporting, and FortiData dashboard to prioritize visibility and alerting based on data sensitivity to the organization. FortiData extends data visibility to:

- On-premise data stores (SMB/CIFS file systems)
- AWS S3 Buckets
- Microsoft SharePoint Online data stores
- SharePoint on-premise

### Data Security Posture Management

FortiData goes beyond discovery, classification, and labeling of sensitive data to centralize data visibility and provide administrators and leaders with an assessment of the current state of their organization's data security posture. At a summary level, administrators can quickly identify areas for further review across data types or data labels—and drill down further for deeper analysis and investigation.

FortiData gives administrators powerful functionality for discovering, classifying and tagging data associated with compliance, security, and privacy frameworks in place around the world. With 220+ predefined data templates tied to frameworks, administrators can customize scans for detecting data based on the specific frameworks that matter to their organizations. Meanwhile, administrators can quickly see what sensitive data exists and where at an executive view or drill down into specific repositories, classification labels, and files.

[illegible]

## Key Features



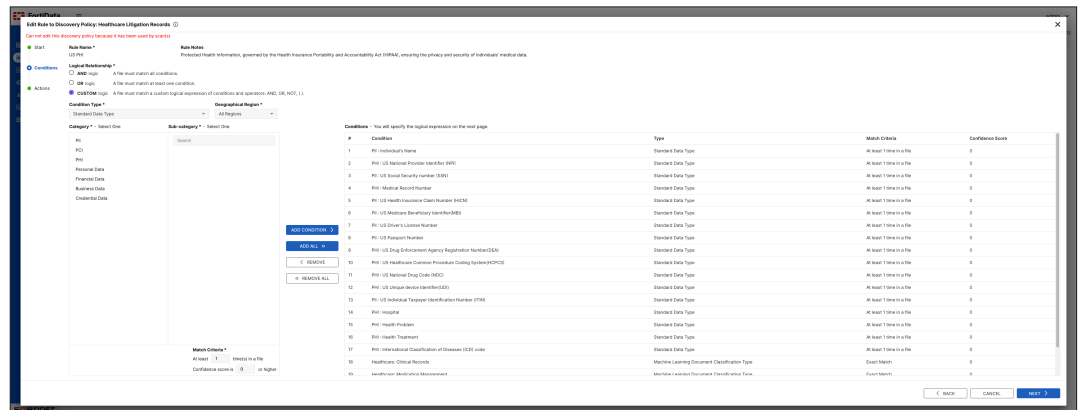
- Performs data discovery, data classification, labeling, and data security posture visualization and management
- Uses advanced machine learning algorithms to fingerprint and scan files for sensitive structured and unstructured content whether the data is stored in the cloud (Microsoft SharePoint Online or AWS S3 buckets) or on-premises data stores (SMB/CIFS file systems and Microsoft SharePoint on-premises)
- Allows administrators to apply predefined or custom data labels to sensitive data
- Helps organizations comply with data requirements associated with major compliance frameworks
- Provides a centralized single-pane-of-glass view of an organization's data security posture
- Enables stronger data loss prevention across the Fortinet Security Fabric through integrations and sharing of data classification labels
- Customers can protect data at rest, in use, and in transit through utilization of Fortinet Security Fabric data protection offerings and services

## Use Cases

### Data Discovery

FortiData performs data discovery across both on-premises (those using SMB/CIFS file systems and Microsoft SharePoint on-premises) and cloud-based data stores (Microsoft SharePoint Online and AWS S3 buckets).

Administrators can configure rules for scanning of data stores across their organization's hybrid environment. They can also develop scans for specific types of data based on the FortiData extensive library of dictionaries.



### Data Classification

FortiData applies machine learning and natural language processing technologies to optimize classification of sensitive data types including PII, PHI, PCI data, financial data, intellectual property, and code. Administrators can classify data based on predefined or custom labels. In addition, FortiData utilizes industry-specific trained data models for sensitive data types typically associated with Financial, Education, Healthcare, Information Technology, and Manufacturing industries.

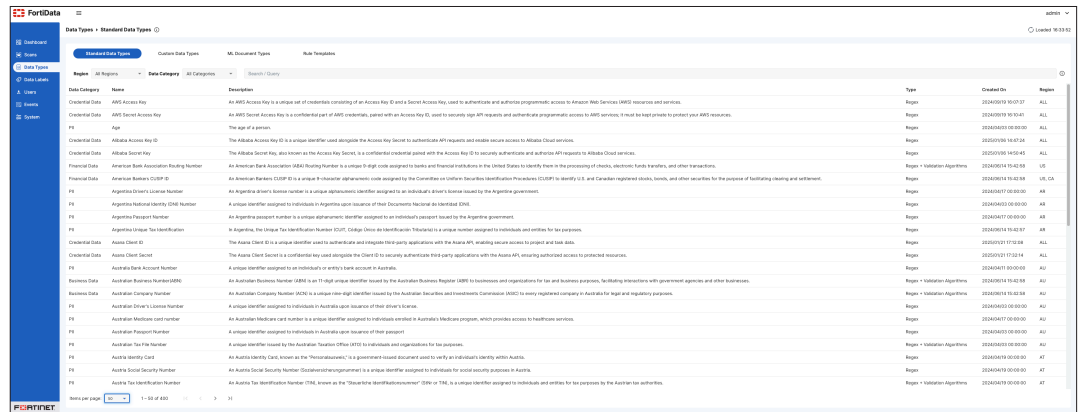
### Data Security Posture Management

FortiData provides centralized visibility through a single-pane-of-glass dashboard view into the current state of organization's data security posture. Administrators can prioritize by data type to get an immediate sense of what data exists, the nature of that data, where it exists, and can drill down for more insights and review.

## Comprehensive Regulatory and Industry Framework Coverage

FortiData helps Security and IT administrators comply with and report on adherence to data protection requirements associated with major compliance frameworks.

FortiData includes 220+ predefined data templates addressing data types associated with compliance, security and privacy frameworks. These templates allow organizations to identify and label appropriate sensitive data (PII, PHI, PCI cardholder data, and more) per a myriad of security and privacy frameworks including PCI DSS, HIPAA, CCPA, GDPR, ISO 27001, SOC 2, GLBA, SOX, and other frameworks spanning countries around the world.



Region	All Regions	Data Category	All Categories	Search / Filter	Name	Description	Type	Created On	Region
Cloud Data					Amazon Access Key	An AWS Access Key is a unique set of credentials consisting of an Access Key ID and a Secret Access Key, used to authenticate and authorize programmatic access to Amazon Web Services (AWS) resources and services.	Region	2024/09/19 00:07:37	ALL
Cloud Data					AWS Secret Access Key	An AWS Secret Access Key is a confidential part of AWS credentials, paired with an Access Key ID, used to securely sign API requests and authorize programmatic access to AWS services. It must be kept private to protect your AWS resources.	Region	2024/09/19 00:07:41	ALL
Cloud Data					Age	The age of a person.	Region	2024/09/19 00:00:00	ALL
Cloud Data					Alibaba Access Key ID	The Alibaba Access Key ID is a unique identifier used alongside the Access Key Secret to authenticate API requests and enable secure access to Alibaba Cloud services.	Region	2025/09/19 00:07:34	ALL
Cloud Data					Alibaba Secret Key	The Alibaba Secret Key, also known as the Access Key Secret, is a confidential credential paired with the Access Key ID to securely authenticate and authorize API requests to Alibaba Cloud services.	Region	2025/09/19 00:07:45	ALL
Financial Data					American Bank Association Routing Number	An American Bank Association (ABA) Routing Number is a unique 9-digit code assigned to banks and financial institutions in the United States to identify them in the processing of checks, electronic funds transfers, and other transactions.	Region + Validation Algorithm	2024/09/19 00:00:00	US
Financial Data					American Bankers (CIS) ID	An American Bankers (CIS) ID is a unique 8-character alphanumeric code assigned to the financial institutions participating in the American Bankers Association (ABA) system to identify U.S. and Canadian registered clients, banks, and other securities for the purpose of facilitating clearing and settlement.	Region	2024/09/19 00:00:00	US, CA
Financial Data					Argentina Driver's License Number	An Argentine Driver's License Number is a unique alphanumeric identifier assigned to an individual's driver's license issued by the Argentine government.	Region	2024/09/19 00:00:00	AR
Financial Data					Argentina National Identity (DNI) Number	A unique identifier assigned to individuals in Argentina upon issuance of their Documento Nacional de Identidad (DNI).	Region	2024/09/19 00:00:00	AR
Financial Data					Argentina Passport Number	An Argentine passport number is a unique alphanumeric identifier assigned to an individual's passport issued by the Argentine government.	Region	2024/09/19 00:00:00	AR
Financial Data					Argentina Unique Tax Identification	In Argentina, the Unique Tax Identification Number (CUIT, Cédula Única de Identificación Tributaria) is a unique number assigned to individuals and entities for tax purposes.	Region	2024/09/19 00:00:00	AR
Cloud Data					Azure Client ID	The Azure Client ID is a unique identifier used to authenticate and authorize client applications with the Azure AD, enabling secure access to Azure and SaaS apps.	Region	2025/09/19 00:00:00	ALL
Cloud Data					Azure Client Secret	The Azure Client Secret is a confidential key used alongside the Client ID to securely authenticate third-party applications with the Azure AD, ensuring authorized access to protected resources.	Region	2025/09/19 00:00:00	ALL
Cloud Data					Australia Bank Account Number	A unique identifier assigned to an individual's or entity's bank account in Australia.	Region	2024/09/19 00:00:00	AU
Business Data					Australian Business Number (ABN)	An Australian Business Number (ABN) is an 11-digit unique identifier issued by the Australian Business Register (ABR) to businesses and organizations for tax and business purposes, facilitating interactions with government agencies and other businesses.	Region + Validation Algorithm	2024/09/19 00:00:00	AU
Business Data					Australian Company Number	An Australian Company Number (ACN) is a unique nine-digit identifier issued by the Australian Securities and Investments Commission (ASIC) to every registered company in Australia for legal and regulatory purposes.	Region + Validation Algorithm	2024/09/19 00:00:00	AU
Business Data					Australian Driver's License Number	A unique identifier assigned to individuals in Australia upon issuance of their driver's license.	Region	2024/09/19 00:00:00	AU
Business Data					Australian Medicare card number	An Australian Medicare card number is a unique identifier assigned to individuals enrolled in Australia's Medicare program, which provides access to healthcare services.	Region	2024/09/19 00:00:00	AU
Business Data					Australian Passport Number	A unique identifier assigned to individuals in Australia upon issuance of their passport.	Region	2024/09/19 00:00:00	AU
Business Data					Australian Tax File Number	A unique identifier issued by the Australian Taxation Office (ATO) to individuals and organizations for tax purposes.	Region + Validation Algorithm	2024/09/19 00:00:00	AU
Business Data					Austria Identity Card	An Austria Identity Card, known as the "Personalausweis", is a government-issued document used to verify an individual's identity within Austria.	Region	2024/09/19 00:00:00	AT
Business Data					Austria Social Security Number	An Austria Social Security Number (Sozialversicherungsnummer) is a unique identifier assigned to individuals to participate in social security programs in Austria.	Region	2024/09/19 00:00:00	AT
Business Data					Austria Tax Identification Number	An Austria Tax Identification Number (UID, known as the "Steuerliche Identifikationsnummer") is a unique identifier assigned to individuals and entities for tax purposes by the Austrian tax authorities.	Region + Validation Algorithm	2024/09/19 00:00:00	AT



## Order Information

Available in a Virtual Machine:

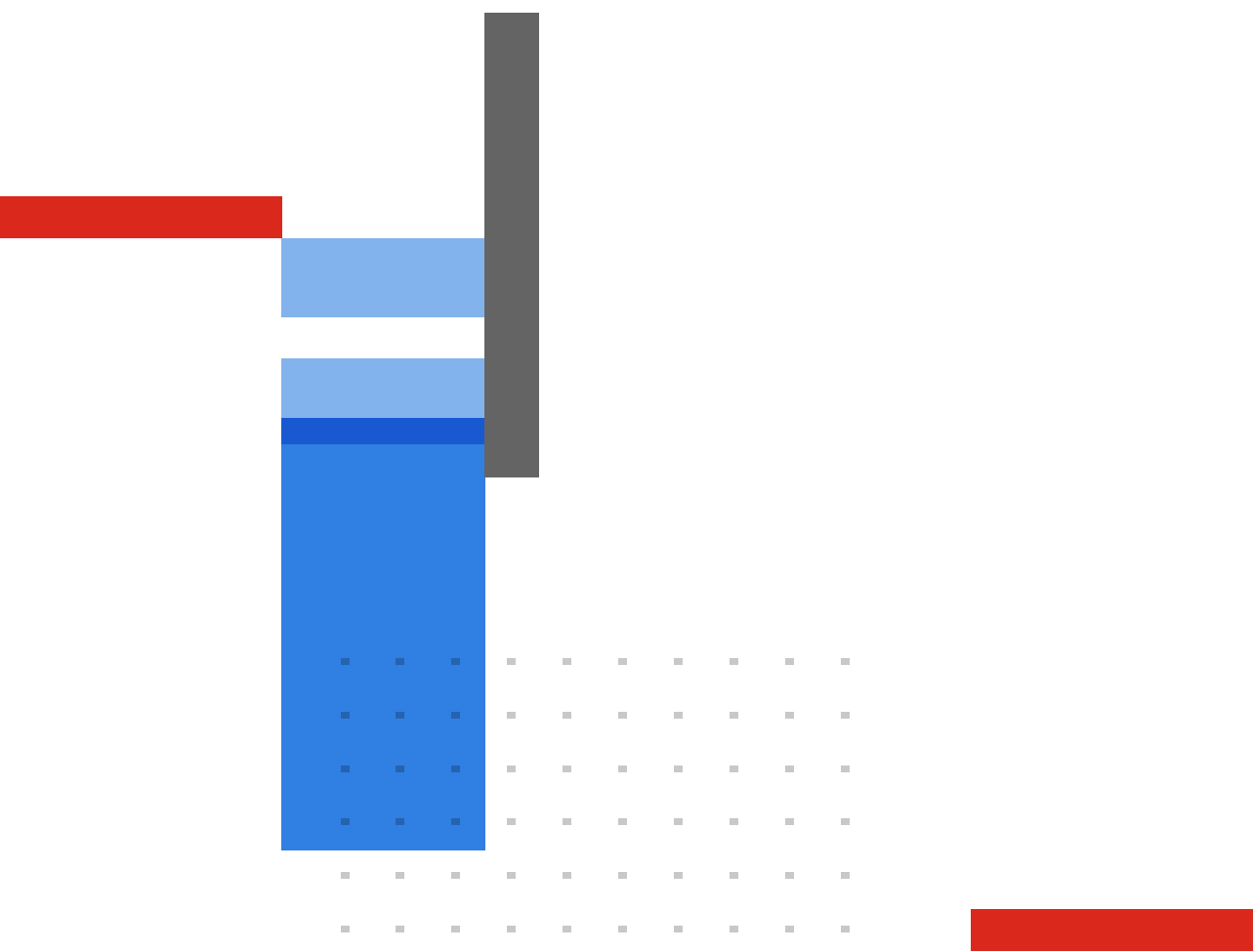
- 16 and 32 virtual CPU options
- Supports ESX and KVM deployments

SKU	Description
FC1-10-DTVMS-248-02-DD	FortiDATA VM Subscription License SKU - 1 Year. VM with 16 cores and 32 GB memory.
FC2-10-DTVMS-248-02-DD	FortiDATA VM Subscription License SKU - 1 Year. VM with 32 cores and 64 GB memory

Visit <https://www.fortinet.com/resources/ordering-guides> for related ordering guides.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the [Fortinet EULA](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).



www.fortinet.com

Copyright © 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.