

SOLUTION BRIEF

# BlueXP classification (Cloud Data Sense)



**Discover and classify your data for enhanced governance and privacy.**

BlueXP classification gives you actionable insights into your data to address compliance requirements, detect security vulnerabilities, optimize costs, and accelerate cloud migration.

## Do you know where all of your data is, what kind of data you have, and who can access it?

Most organizations can't answer "YES" to this question. If, for example, you needed to find all personal or sensitive company data that is unintentionally exposed to the public, how would you do that? What if you were asked to run a Data Subject Access Request report to comply with customer requests and the law? What if you wanted to remove all stale, duplicate, and non-business files before migrating data sets to the cloud so you don't waste budget moving and storing unneeded data? How would you do it today?

There's more data being generated than ever, and much of that data lives outside of the on-premises data center in clouds, edge locations, and in hybrid, multicloud, heterogeneous environments. Storing it increases compliance and cybersecurity risks and, of course, costs. How can you organize and manage your data appropriately so it's cost-effective, secure, and compliant with regulations? It's a big job. And without a modern approach to data governance, it's likely an impossible job.

With NetApp® BlueXP™ classification, you have constant visibility of the data residing in your entire storage footprint no matter where the data physically resides, so that you can optimally control and govern it.

NetApp BlueXP classification is a data governance and classification service delivered via BlueXP that provides insight and reporting for both on-premises and cloud storage across a wide array of types and vendors.

With the simplicity of NetApp BlueXP classification, you empower your IT, storage, data privacy, and compliance teams to do their jobs in the most efficient way. You free up their time for tasks that matter. NetApp BlueXP classification sets a new standard for implementing your organization's data privacy and governance programs with built-in artificial intelligence (AI)-driven privacy controls and easy-to-use Governance and Compliance dashboards. Provided through the NetApp BlueXP unified control plane, BlueXP classification provides a SaaS experience without your data ever leaving your network.

### **Govern all of your data.**

- Control data and perform data hygiene tasks holistically across hybrid, heterogeneous data estates containing multiple technologies and storage solutions.
- Optimize storage and reduce costs by:
  - Archiving stale data
  - Identifying and removing duplications

### **Accelerate cloud migration projects.**

- Map data for migration.
- Identify sensitive data before moving to the cloud.

### **Improve your security posture.**

- Identify open permissions.
- Fuel data ownership/least privileges projects.

### **Maintain regulatory compliance.**

- Map personally identifiable information (PII).
- Comply with privacy regulations, including GDPR, CCPA, PCI, HIPAA.
- Respond quickly to Data Subject Access Requests (DSARs).

Figure 1 NetApp BlueXP classification use cases

## Make intelligent data decisions in real time

BlueXP classification provides automated data governance by mapping the data footprint across hybrid and multicloud landscapes, determining how much data exists, where it is, what type, and the profile of the data. This allows intelligent decisions to be made on data in real time, enabling rapid manual or automated actions to immediately optimize cost and reduce risk.

### Data mapping and optimization

With BlueXP classification you can:

- Map all data from a governance dashboard for insight into all the enterprise's storage.
- Map duplicate data to identify data redundancy for optimization insights.
- Map stale data to clearly understand what data might not be needed anymore.
- Map data not related to the business for cost savings.

- Map data from multiple environments to get a full understanding of all storage (including NetApp and non-NetApp storage, files, objects, and databases).
- Map personal, nonpersonal, and sensitive data for a clear understanding of files that might need stricter permissions.

### Securing sensitive data

With BlueXP classification, you can automatically identify all the files with open permissions and take action to correct the vulnerabilities. You can also ensure that if anything is out of the norm, you will be notified by email about sensitive data that needs to be secured and anomalies that need attention.

### File types

BlueXP classification takes the data that it scans and breaks it down by file type. Reviewing your file types can help you control your sensitive data, because you might find that certain file types are not stored correctly.

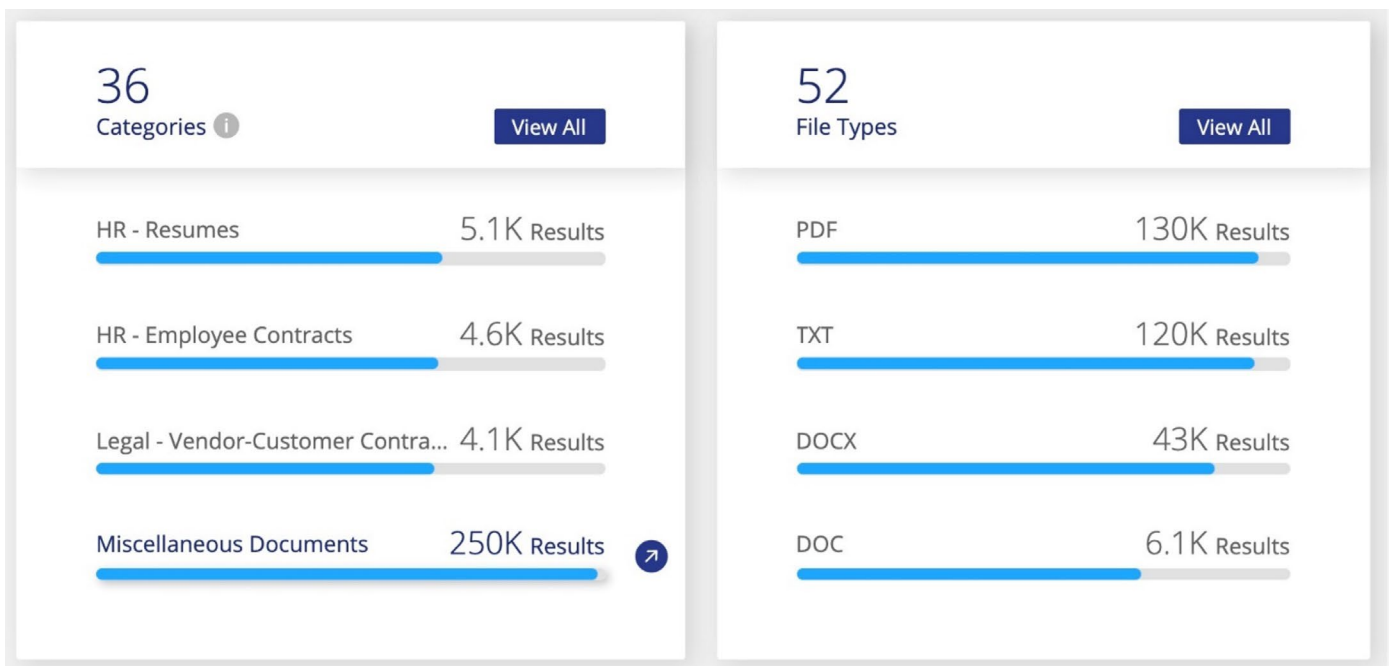


Figure 2 BlueXP classification data mapping

# Quickly uncover compliance and security risks

## Data discovery and classification

BlueXP classification maps and manages sensitive information.

Identifying sensitivities is complex. BlueXP classification uses AI, machine learning (ML), and natural language processing (NLP) technologies to categorize and classify the data as to sensitivity and compliance type, constantly highlighting potential cyber and/or compliance exposures.

Sensitive data is especially important in enterprise environments. Often the sensitivity is specific to the organization (and potentially in a specific domain or language). To define sensitivities accurately, modern AI is a must. BlueXP classification does a lot more than traditional pattern matching and identifies many types of sensitivities.

## Personal data

BlueXP classification automatically identifies specific words, strings, and patterns in the data.

BlueXP classification can recognize PII, credit card numbers, social security numbers, bank account numbers, and more. You can view the full list of private identifiers on the [BlueXP classification website](#).



## PII Distribution

69%  
Non-Sensitive

14%  
Personal

17%  
Sensitive Personal



Figure 3 NetApp BlueXP classification sensitive data classification

BlueXP classification uses proximity validation to validate its findings. The validation works by looking for one or more predefined keywords near the personal data that was found.

For example, BlueXP classification identifies an Australian Tax File Number (TFN) as a TFN only if it finds a proximity phrase next to it— for example, “TFN” or “Tax File.”

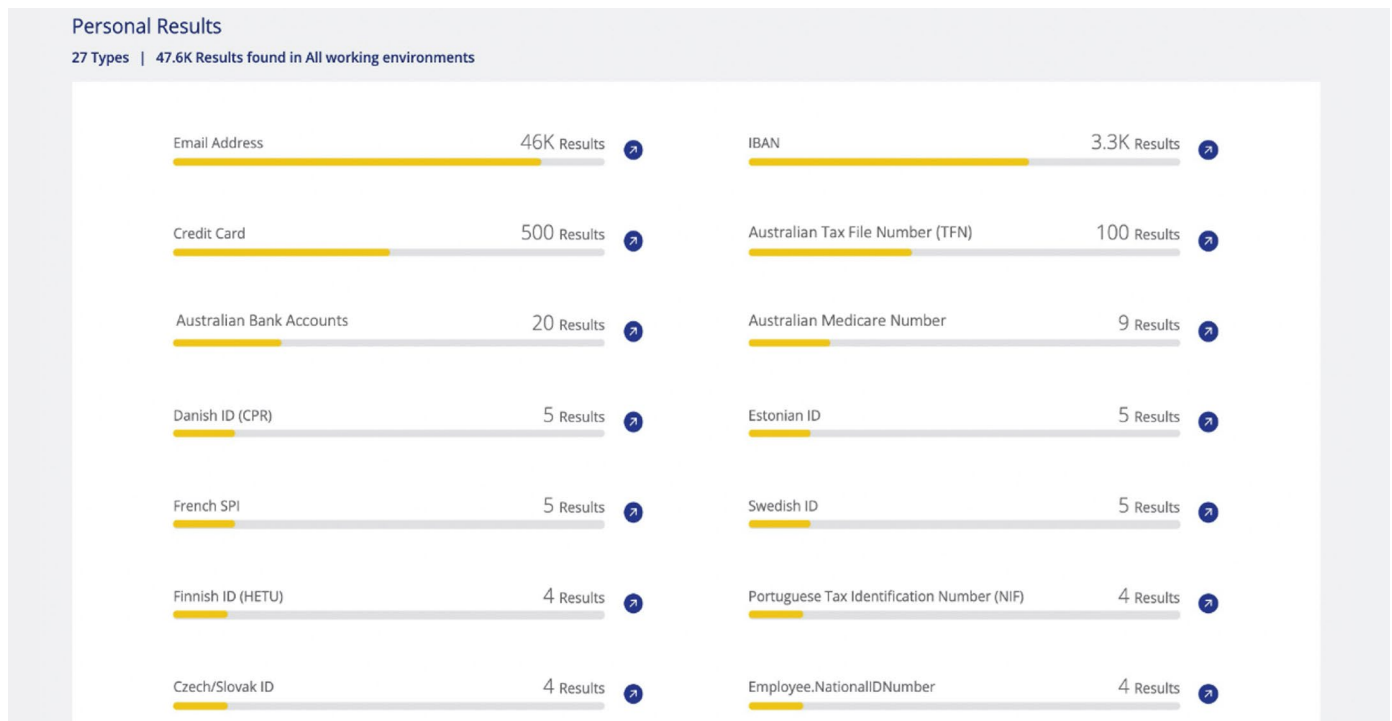


Figure 4 BlueXP classification personal data mapping

## Categories

BlueXP classification takes the data that it scanned and divides it into categories. Categories are topics based on AI analysis of the content and metadata of each file.

Categories can help you understand what's happening with your data by showing you the types of information that you have. For example, a category like résumés or employee contracts can include sensitive data. When you investigate the results, you might find that employee contracts are stored in an insecure location. You can then correct that issue.

## Sensitive personal data

BlueXP classification automatically identifies special types of sensitive personal information, as defined by privacy regulations such as articles 9 and 10 of the General Data Protection Regulation (GDPR).

For example, information regarding a person's health, ethnic origin, or sexual orientation is sensitive personal data.

BlueXP classification understands the content that it scans in order to extract entities and categorize the content accordingly.

For example, one sensitive GDPR data category is ethnic origin. Because of its NLP abilities, BlueXP classification can distinguish the difference between a sentence that reads "George is Mexican" (indicating sensitive data as specified in article 9 of the GDPR), versus "George is eating Mexican food."

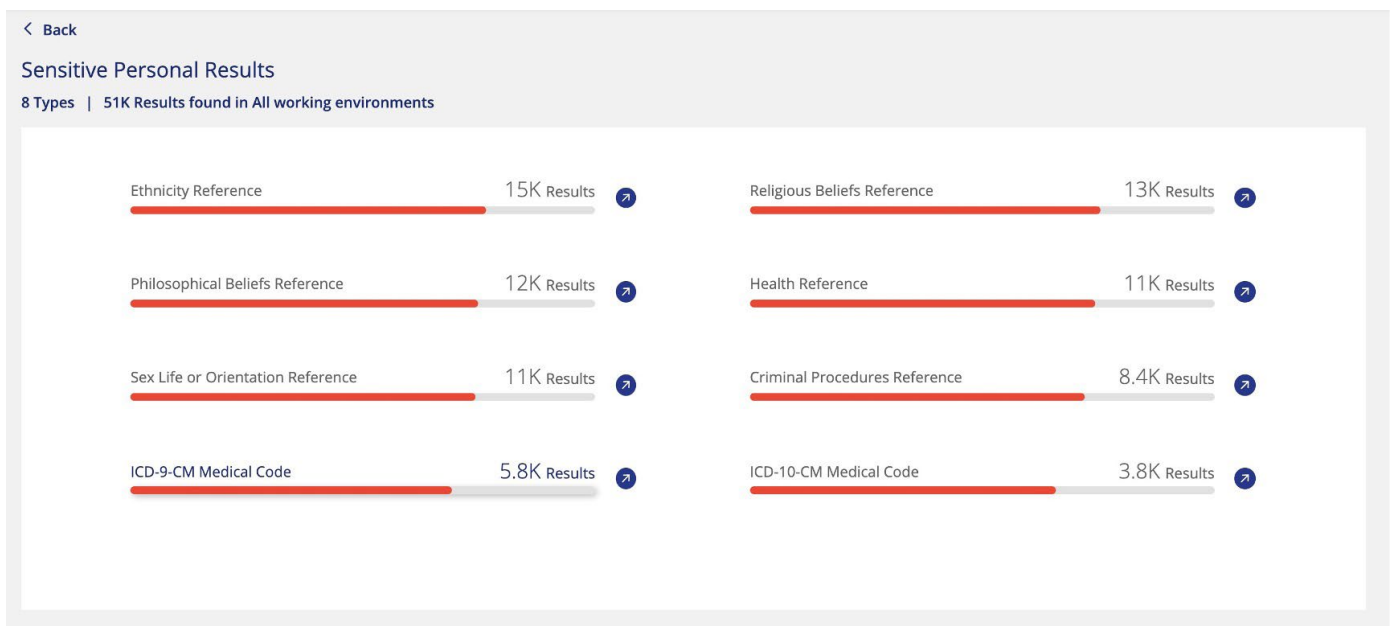


Figure 5 BlueXP classification sensitive personal data mapping

## Service Data Subject Access Requests in minutes

With BlueXP classification, you can respond to a DSAR by searching for a subject's full name or known identifier (such as an email address) and then downloading a report.

The downloaded report can help your organization comply with GDPR or similar data privacy regulations. When you perform a data subject search, BlueXP classification finds the files that have that person's name or identifier in it. After the search is complete, you can then download the list of files for a DSAR report. The report aggregates insights from the data and puts them into legal terms that you can send to the auditor or person/subject.

## Analyzing your privacy program

To help you slash the manual time, cost, and risk of error to achieve compliance parameters, BlueXP classification provides pre-formatted, legally compliant, and customized reports to address a number of compliance and reporting scenarios, including:

### Privacy Risk Assessment Report

The Privacy Risk Assessment Report provides an overview of your organization's privacy risk status, as required by privacy regulations such as GDPR and the California Consumer Privacy Act (CCPA).

### PCI DSS Report

The Payment Card Industry Data Security Standard (PCI DSS) Report can help you identify the distribution of credit card information across your files.

### HIPAA Report

The Health Insurance Portability and Accountability Act (HIPAA) Report can help you identify files containing health information. It is designed to aid in your organization's requirement to comply with HIPAA data privacy laws.

**“NetApp offers a formidable set of business capabilities with unmatched regulatory compliance management, a comprehensive data source support, a contextual AI engine that automatically categorizes data based on context understanding, and support of NetApp’s rich on-premises and cloud-based ecosystem.”**

GigaOm 2022

Top reasons to use NetApp BlueXP classification:

- **Gain visibility:** Get an up-to-date view of the kinds of data that make up your storage footprint — all from one dashboard
- **Stay secure:** Check that no sensitive data has the wrong permissions or is exposed to the wrong people
- **Save money:** Optimize storage costs by identifying, moving, and/or deleting duplicate, stale, and irrelevant data
- **Stay aware:** Alert in real-time on existing and emerging risks
- **Be prepared:** Organize and cleanse data before a data migration project
- **Stay compliant:** Automate time-consuming compliance reporting for PCI, HIPAA, GDPR, CCPA, and more

---

### About NetApp

In a world full of generalists, NetApp is a specialist. We're focused on one thing, helping your business get the most out of your data. NetApp brings the enterprise-grade data services you rely on into the cloud, and the simple flexibility of cloud into the data center. Our industry-leading solutions work across diverse customer environments and the world's biggest public clouds.

As a cloud-led, data-centric software company, only NetApp can help build your unique data fabric, simplify and connect your cloud, and securely deliver the right data, services and applications to the right people—anytime, anywhere. [www.netapp.com](http://www.netapp.com)



+1 877 263 8277