

Data-Centric Security Coming of Age, Enabled with Automation

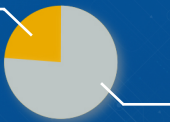
April 2021

Written by: Frank Dickson, Program Vice President, Cybersecurity Products

Report Highlights

Data-centric security has progressed exponentially in the last couple of years, replacing manual tasks with automation. Its key focus is securing the data rather than the infrastructure. Traditional data security solutions were hard to use and difficult to implement, created friction with end-users, and produced inconsistent results. There is also a constant data chase due to sensitive data residing across on-premises and cloud applications, carrying different risk levels and approaches to mitigate the risk to critical data. So how to go about implementing data-centric security? Where to start? IDC recommends three use cases and why data security in the modern workplace is all about easy-to-use tools.

25%
of sensitive data resides in on-premise datacenters



75%
of sensitive data is spread across laptops, desktops, smartphones, public and private cloud environments

30 - 35%
Approx.

Data is Encrypted by IT security practitioners across North America and Europe



Tracking and controlling sensitive data is difficult

```
1 1 0 1 1 1 0 1 1 0 0 1 1 1 1
0 0 0 1 1 0 0 1 0 1 0 1 1 0 1
1 1 1 0 0 0 0 1 1 0 1 0 1 0 1
0 1 0 1 1 1 0 1 1 1 1 1 1 1 1
```

More than 64% of data is very sensitive or extremely sensitive

Data Chase and Struggle

Determining the correct rights & policies to apply



Deciding what to protect



Updating rights when roles change

Making sense of audit and telemetry data



Yesterday's Reality

Modern Approach

Deciding What to Protect : **Visibility is the Key**

User Friction

End users used to get involved in the process of identifying and classifying data



Automating Data Visibility

DLP and cloud security gateway solutions can be automated to work seamlessly with a digital rights management (DRM) solution

Determining the Correct Rights and Policies: **Application Accuracy**

Manual Privacy Methods

Organizations placed data security controls on data that did not need them and not protect intellectual property (IP) that needed it



Accurate Automation of Security Policy

A PrivacyOps framework is required, which enables individual-level data intelligence and layers of automation in a collaborative environment for various stakeholders

Updating Rights When Roles Change: **Just-In-time Agile Application**

Manual Process

Changing security policies was a manual process that relied on the end user and/or administrator intervention



Automation of the Identity Life Cycle to Data-Centric Security

By automating role-based data access controls in real time, companies can easily adjust to an increasing complex set of data sovereignty and control issues

Making Sense of Audit and Telemetry Data: **Data-Centric Intelligence**

Expensive and Non-scalable

Yesterday's approach of having specialists in security, privacy, and/or compliance do the work is expensive and not scalable; asking end users to attempt it is simply inefficient



Leveraging Automation and Artificial Intelligence

Automation and machine intelligence have created transparent data visibility and control. Time to value is reduced, and enterprises can get to security fast and easy

Where to Start ?

IDC recommends focusing on use cases that provide the maximum value for data protection initiatives to achieve early wins and enable a foundation for continued success. Three use cases commonly stand out for a big return on initial investments are:



Collaboration and email



External collaboration



Extending DLP and cloud security gateways

Data Security in the Modern Workplace

It is all about tools and how quick and easy you can get them running



The volume of enterprise data creation and acquisition typically increases at a compound annual growth rate of 40-50%



Data security tools must be easy to implement and use



The long-standing control objectives of data confidentiality, integrity, and availability are important components to a data protection security strategy