NEXTLABS®

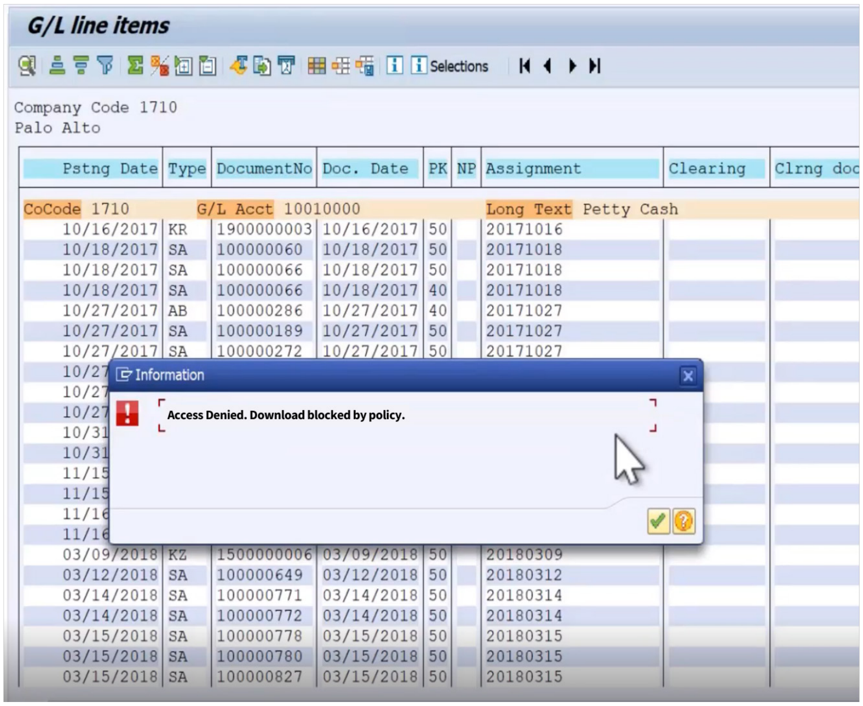
Data Loss Prevention for SAP ERP

Protect Data at Rest, in Use, and On the Move

OVERVIEW

As one of the most widely used enterprise software, SAP applications encompass critical aspects of business operations, ranging from CRM and ERP to financial transactions and supply chain management. The sensitive data contained within the SAP applications are under increasingly rampant threats of data loss. Externally, researchers discovered a 400% increase in ransomware incidents that involved compromising the SAP systems and data in recent years. Internally, dispersed workforce and extended collaboration landscape increased the risks of accidental data leakage.

It is vital to safeguard sensitive information in SAP by monitoring, controlling, and securing data in motion, at rest, and in use. Unauthorized export, extraction, download, or accidental loss of sensitive data must be prevented through implementing policies that identify and block risky activities. Tools need to analyze data patterns, detect confidential content, and enforce restrictions based on predefined rules. This proactive approach minimizes the risk of data loss.



Company Code 1710
Palo Alto

Pstng Date	Type	DocumentNo	Doc. Date	PK	NP	Assignment	Clearing	Clrng doc
CoCode 1710		G/L Acct 10010000				Long Text Petty Cash		
10/16/2017	KR	1900000003	10/16/2017	50		20171016		
10/18/2017	SA	100000060	10/18/2017	50		20171018		
10/18/2017	SA	100000066	10/18/2017	50		20171018		
10/18/2017	SA	100000066	10/18/2017	40		20171018		
10/27/2017	AB	100000286	10/27/2017	40		20171027		
10/27/2017	SA	100000189	10/27/2017	50		20171027		
10/27/2017	SA	100000272	10/27/2017	50		20171027		
10/27								
10/27								
10/27								
10/31								
10/31								
11/15								
11/15								
11/16								
11/16								
03/09/2018	KZ	1500000006	03/09/2018	50		20180309		
03/12/2018	SA	100000649	03/12/2018	50		20180312		
03/14/2018	SA	100000771	03/14/2018	50		20180314		
03/14/2018	SA	100000772	03/14/2018	50		20180314		
03/15/2018	SA	100000778	03/15/2018	50		20180315		
03/15/2018	SA	100000780	03/15/2018	50		20180315		
03/15/2018	SA	100000827	03/15/2018	50		20180315		

Access Denied. Download blocked by policy.

The imperative to guard against external and internal threats calls for a fine-grained and flexible solution that protects SAP data regardless of where it resides throughout its lifecycle. This is a scenario where a Data Loss Prevention solution can help. DLP is a combination of methods and technologies that categorize, identify, and safeguard sensitive data against unauthorized extraction, download, or loss. Organizations must implement a DLP solution to avoid the consequences of data leakage in SAP applications, and potentially disastrous results.

THE SOLUTION

DLP for SAP ERP leverages SAP's classifications and information about users and utilizes attribute-based policies to enforce proper authorization at runtime. The policies are managed centrally making changing policies much easier with the ability to enforce consistently across a variety of applications.

DLP for SAP ERP automates protection, applying segregation, filtering, and obfuscation when data is accessed in a data source. In addition, DLP for SAP ERP uses policies to prevent unauthorized extraction or download of protected data, enforcing the principle of least privilege access to the data, only allowing the minimal rights (e.g. read but not export) that are necessary for a user or entity to complete their task. All data access requests are logged and monitored centrally, to ensure that data loss is prevented across the entire enterprise.

KEY FEATURES

KEY FEATURES	
Data Leak Prevention	Prevent data leakage from all exit points of the SAP ERP and PLM Applications
Centralized Policy Management	Prevent unauthorized extraction of sensitive data based on a centrally managed policy
Centralized Audit and Monitoring	Monitor and log the extraction of critical data based on policy
Automated Data Classification	Automatically tag files containing data extracted from the SAP ERP or PLM application with user, persona, transaction, classification, and business object attributes
Native SAP Integrations	Integrate natively with SAP GUI, SAP ECC, and SAP S/4HANA
Support for Third-Party DLP Solutions	Support integrations with third-party DLP solutions and Microsoft Azure Information Protection (AIP)
Centralized Visibility	Centralized monitoring and reporting on data use for full visibility
Block Uploads	Prevent uploads of data to SAP ERP and PLM systems that do not conform to policy

ABOUT NEXTLABS

NextLabs®, Inc. provides zero trust data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based zero trust policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, AWS, Accenture, Deloitte, Infosys, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.