

Dow

Chemicals



## OVERVIEW

- 120 years of combining science and technology to drive innovation
- More than 6,000 product families
- Customers in 180 countries
- \$48 billion in revenue
- 56,000 employees worldwide

## DOW'S STORY

Dow manufactures a variety of products that are subject to export control regulations in the US, and other countries around the world. The company has an export control group to maintain export data, license determinations, and record keeping, but its manual procedures chiefly, spreadsheets were time-consuming, costly, and potentially error-prone. When a user wanted access to technical data that was classified as an export control item, manual approvals on a user-by-user basis were the norm. Given the sheer size and scope of Dow's global operations, it needed a way to automate and enforce export control policies consistently across the enterprise. When it came to intellectual property (IP), which is the lifeblood of Dow's innovative product line, the company needed a way to securely share technical data with third parties. It needed protection of IP at the data level, regardless of where and how the data was shared.

## THE CHALLENGE

In the US, any company that distributes physical goods, services, technology, software or technical data to foreign nationals or countries is required to comply with export control regulations, and violators may be subject to monetary damages, loss of export privileges, and even imprisonment in some cases. Besides the US export control regulations—International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR)—Dow is also subject to regulations in the countries it's exporting to, such as German BAFA, UK Export Control Act, and EU Dual Use Regulations.

Dow manufactures more than 6,000 product families at 179 sites in 35 countries across the globe. Satisfying export regulations across such a broad global footprint, and across multiple jurisdictions, is a major challenge. Adding to the complexity are its global operations, mobile workers, offshore subsidiaries, joint ventures, and extensive partner or supply collaboration networks. Manual processes simply can't keep up.

As a company that combines science and technology to create new revenue streams, Dow also has a critical need to secure its IP—not only from external threat but also from internal misuse or carelessness. Because Dow needs to share IP with external suppliers and with potential partners in joint ventures, the challenge of protecting IP across the Dow ecosystem is quite complex.

## ROLE-BASED SECURITY ADDS COMPLEXITY

Dow had been using role-based access control (RBAC) to protect export data and intellectual property. But as its business expanded and the "extended enterprise"—the ecosystem of customers, devices, clouds, partners, supply chains, and users that companies now work within—became more complex, the role-based approach became difficult to maintain and troubleshoot. Consider this: every time a new variable is introduced (such as a new geographical location or a new data class), the company needs a new set of roles to handle each new variable. The administration of tens of thousands and even hundreds of thousands of roles is resource intensive and serves to slow down business processes – limiting agility and responsiveness.

## CUSTOM DEVELOPMENT IS EXPENSIVE AND INFLEXIBLE

Dow has been an SAP customer for more than 20 years. The company was no stranger to custom development to enhance its multiple SAP instances, and it considered doing manual extensions to ERP to enable more fine-grained authorization of technical data. However, solutions based on custom authorization are expensive to operate and maintain, and can potentially expose a company to compliance risk. Short-term fixes may block future business objectives. And most importantly, will a customized authorization solution provide adequate confidence that punitive export control and IP protection requirements are fully met?

## THE SOLUTION

What Dow needed was fine-grained access control that would protect technical data from being accessed without authorization, while still allowing users to do their jobs. Dow also wanted a commercial off-the-shelf (COTS) solution, in order to benefit from faster deployment, increased operational efficiency, and lower total cost of ownership (TCO). Its requirements were to:

- Automate manual procedures for maintaining technical export, license determination, and record keeping
- Implement automated export control processes across multiple jurisdictions with complex export authorizations
- Provide granular access control to protect controlled technical data within SAP
- Monitor and control the sharing of Dow IP with third parties or potential joint-venture partners
- Create access and usage reports for all controlled technical data

Dow chose NextLabs Application Enforcer for SAP, which integrates out of the box with SAP ERP Core Component (ECC), to ensure export compliance and securely protect its intellectual property. NextLabs Application Enforcer dynamically evaluates authorization policies at runtime, based on user attributes (such as citizenship, department, and roles); resource attributes (such as data classification, content, and transaction details); and environment attributes (such as time of day, location, and device type). Real-time evaluation allows the system to use the latest information to determine if access should be granted. Administrators at Dow no longer need to maintain and keep track of role and permission assignments as users move between departments, projects, or locations.

Simple policy changes can reflect new business requirements which are enforced consistently across the enterprise. NextLabs is automatically aware of these changes and ensures that access is restricted or allowed based on the current environment.

## RESULTS

By centralizing policy management and extending SAP's role-based authorization with attribute-based controls, Dow has been able to:

- Protect SAP data wherever it is used, whether inside or outside the organization
- Streamline and automate data classification based on its predefined rules, keywords, and metadata
- Provide fine-grained, contextual access control based on attributes such as nationality and location and other relevant factors
- Provide an audit trail and compliance reporting on usage/access of protected technical data

## SYSTEM BENEFITS

With its deployment of NextLabs Application Enforcer for SAP, Dow is enjoying the following features and benefits:

Feature	Benefit
Attribute-Based Access Control	<ul style="list-style-type: none"><li>• Control access to technical data</li><li>• Prevent contamination and unauthorized disclosure</li></ul>
Data Classification	<ul style="list-style-type: none"><li>• Easily label technical data</li><li>• Protect technical data end-to-end</li></ul>
Centralized Policy Management	<ul style="list-style-type: none"><li>• Centralized control of global policy sets</li><li>• Leverage SAP GTS export license for policy decisions</li></ul>
Automation and Remediation	<ul style="list-style-type: none"><li>• Automate user assistance and remediation</li><li>• Raise user awareness with policy messages</li></ul>
Comprehensive Audit	<ul style="list-style-type: none"><li>• Track access to technical data</li><li>• Integrate with SAP GTS for compliance reporting</li></ul>

**NEXTLABS<sup>®</sup>** | **Zero Trust  
Data-Centric Security**

## ABOUT NEXTLABS

NextLabs<sup>®</sup>, 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>.