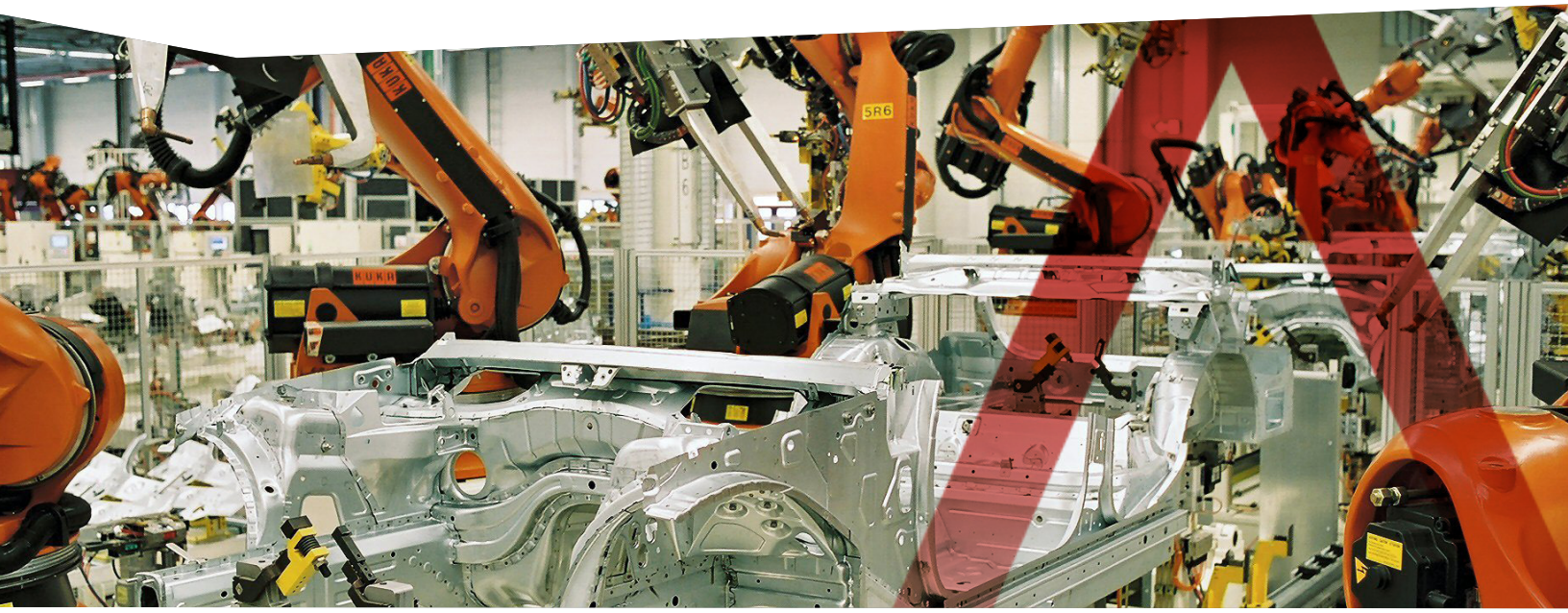
RSA

CASE STUDY



AUTO MAKER REDUCES DATA RETENTION AND ACCESS RISKS WITH RSA® IDENTITY GOVERNANCE AND LIFECYCLE

When it comes to data, many organizations are hoarders: They want as much of it as they can possibly get, knowing that with today's technologies, they can use it to drive more effective analytics, more accurate financial and inventory forecasting, and more innovative marketing programs. As a result, their systems are bursting with petabytes of data.

The problem with this hoarder mentality is that it exposes organizations to a variety of risks, including audit findings, compliance violations, regulatory fines and data breaches—to say nothing of storage costs. Unfortunately, the folks in operations and marketing who wish to collect, store and mine this data are often unaware of these risks, which are growing more serious each day due in large part to GDPR.

This lack of awareness was a problem for a large automotive company, where different departments and functions tended to hold onto data indefinitely, despite internal data retention policies. The company's data governance and retention issues were complicated by access governance issues—specifically, too many people had too much access to data stored in various file shares and systems, which created additional compliance and security risks.

RAISING AWARENESS

In 2011, the auto maker's security operations team undertook two ongoing programs aimed at improving data and access governance and reducing related risks. The data access governance program highlights the different kinds of data stored across the company, including the length of time various pieces of data have been stored. It also focuses on deleting data that's more than seven years old (in accordance with company policy) and

"Built-in workflows make it easier for functional managers to follow best practices for provisioning, de-provisioning and access management."

Security operations manager, *major automotive manufacturer*

CUSTOMER VITAL STATISTICS

Industry: Automotive/Manufacturing

Number of employees: +30,000

RSA product:

- RSA Identity Governance & Lifecycle

Been an RSA customer for: 10 years

What I like about RSA:

- Product works across platforms
- Breadth and depth of product capabilities
- Professional services support
- Flexible deployment and licensing model

cleaning up people's access to file systems. The enterprise access governance program reviews data and access governance issues across financial systems, privileged accounts and some HR systems. The security operations team uses RSA Identity Governance and Lifecycle to support both programs.

RSA Identity Governance and Lifecycle reveals what data is stored where (and which function owns it) and the risk that data creates. It also identifies any kind of access that any single identity has to any kind of system, in addition to highlighting orphaned accounts, segregation of duties violations, privileged access violations and the like. Equally important, RSA Identity Governance and Lifecycle automatically remediates "toxic access" in real time, as soon as it finds problematic access points.

The security operations manager leading these two programs says one of the benefits of RSA Identity Governance and Lifecycle is its ability to work across platforms: It "harvests" metadata from the company's many, varied and disparate applications, systems, directories and file shares; this capability creates a comprehensive picture of access—and risk—across the company. He's also pleased with the solution's discovery capability: "It finds so much, including access issues that may have been created more than a decade ago, before we started using the tool."

CHANGING HEARTS AND MINDS

With the ability to identify data and access enterprise-wide, the security operations team has been working to get functional managers and end users to embrace their role as data stewards. They're also trying to get functional managers to change their overly generous provisioning and nearly non-existent de-provisioning processes.

"That's one of our biggest challenges: empowering the business to embrace new processes and attitudes toward data governance and access management," says the security operations manager. "This is a challenge for many organizations, especially ones with large application portfolios and tens of thousands of employees."

It's a challenge RSA Identity Governance and Lifecycle is built to address. The security operations manager says the solution's built-in workflows make it easier for functional managers to follow best practices for provisioning, de-provisioning and access management.

TOWARD A MORE EFFICIENT IGA PROGRAM

The auto maker has been using RSA Identity Governance and Lifecycle for a decade. During that time, the company has seen RSA evolve continually to support different types of infrastructure and new licensing and deployment models. "We're taking advantage of these changes," says the security operations manager, "and it's helping us run a more efficient identity and access governance program."

> "One of the benefits of RSA Identity Governance and Lifecycle is its ability to work across platforms."
>
> ***Security operations manager,*** *major automotive manufacturer*

ABOUT RSA

RSA® Business-Driven Security™ solutions uniquely link business context with security incidents to help organizations manage digital risk and protect what matters most. With award-winning cybersecurity solutions from RSA, a Dell Technologies business, organizations can detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of Fortune 500 companies thrive in an uncertain, high risk world. For more information, visit rsa.com.

RSA