



FOOD COMPANY CUTS EXCESS PRIVILEGES, REDUCES RISK WITH RSA® IDENTITY GOVERNANCE AND LIFECYCLE

Any company with tens of thousands of employees and contractors working together to manufacture and market dozens of major brands is going to face tough operational challenges every day. For one U.S.-based food company in that situation, a critical consideration has been provisioning and managing its myriad users' access to data, applications and other resources.

For years, the food company relied on in-house applications and manual processes to assign and manage access across the organization. Recently, however, an audit of its Active Directory (AD) and SAP environments revealed some troubling inconsistencies in how those activities were being handled. It quickly became clear the company needed a more effective approach to access reviews and access rights management.

"Making sure the right access has been granted to the right people presents a substantial challenge in such a large, dynamic access environment, where you have so many employees and third-party users constantly coming and going," says the company's senior manager of cybersecurity. "After the audit, we realized having multiple solutions further complicated

CUSTOMER VITAL STATISTICS

Industry: Food Manufacturing

RSA product: RSA Identity Governance and Lifecycle

What I like about RSA:

- One unified platform for access reviews across the company
- Accurate, efficient, automated access certifications
- Ability to easily eliminate unnecessary access
- Streamlined compliance processes and documentation
- Alignment of security requirements and business goals

"Automating all these activities has given us solid improvements in accuracy and efficiency."

Senior manager of cybersecurity

that challenge, and that we needed one unified way to manage access rights across the entire company.”

That’s when the company implemented RSA® Identity Governance and Lifecycle as a centralized platform for conducting access reviews at its businesses and operations around the globe.

IMPROVEMENTS IN ACCURACY, EFFICIENCY AND ACCOUNTABILITY

With RSA Identity Governance and Lifecycle in place, the company has been able to consolidate and automate a multitude of manual access-review processes.

“Automating all these activities has given us solid improvements in accuracy and efficiency,” says the senior manager of cybersecurity. “And having a standardized, company-wide mechanism for handling access certifications has also reduced the risk posture of the organization.”

The reduction in risk posture comes largely from addressing an over-accumulation of access privileges that had been steadily increasing as employees moved around the company. That problem stemmed from a lack of formalized ownership for determining and maintaining access privileges.

Simply put, users had access rights to far more resources than they needed, a risky situation that no one in the organization could fully grasp—given the distributed way those rights were managed—much less figure out how to solve. That changed with the adoption of RSA Identity Governance and Lifecycle.

EXCESSIVE ACCESS PRIVILEGES REDUCED BY 25 PERCENT

In the first access-review cycle after standardizing on RSA Identity Governance and Lifecycle, the company experienced a 25 percent reduction in assigned access rights, a rate that has since stabilized at around 5 percent from semi-annual access reviews.

The initial dramatic drop happened after individual managers began using the RSA solution to assume formal ownership of assigning appropriate access rights. Several specific process improvements came about as a result of this shift:

- Supervisors now perform access certifications semi-annually, focusing on the most sensitive entitlements.
- When an employee moves to a new role, the new manager performs a full access certification to ensure there is no accumulation of unnecessary access.
- Access rights are automatically revoked if a supervisor doesn’t revalidate the needs of a team member in a timely fashion.

The company has also been able to review and take action to ensure that appropriate rights are assigned to contractors as well as employees.

INCREASED COMPLIANCE AND AUDIT EFFICIENCIES

Because the company is publicly traded, compliance is a significant driver in many aspects of its operations. “We knew that by simplifying the process of managing access rights, we could also reduce our compliance burden,” says the senior manager of cybersecurity.

“RSA Identity Governance and Lifecycle enables us to wholly align our efforts in supporting all of the most critical aspects of the business.”

Senior manager of cybersecurity



Using RSA Identity Governance and Lifecycle to drive consistency and accountability has reduced the amount of effort needed to prepare for compliance testing. And because the solution makes it possible to easily ensure that people have access that is appropriate to their role, the entire compliance process is streamlined.

Having a single standardized platform for managing access rights also makes it easier to produce the documentation to verify to auditors that the company is in compliance.

A CATALYST FOR POSITIVE CHANGE

The company's standardization on RSA Identity Governance and Lifecycle has sparked positive changes across the organization that go beyond reducing compliance risk and improving operational efficiency and productivity. Individual groups have seen benefits that include spending less time with auditors and reducing maintenance requirements.

RSA Identity Governance and Lifecycle is also helping the company achieve alignment of security concerns and regulatory responsibilities with business goals. "It's imperative to consider the full access lifecycle and to make sure that you're able to respond to the needs of the business," says the senior manager of cybersecurity. "RSA Identity Governance and Lifecycle enables us to wholly align our efforts in supporting all of the most critical aspects of the business."

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 cyber-crime. 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.



The information in this publication is provided "as is." Dell Inc. or its subsidiaries make no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright 2018 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

Dell Inc. or its subsidiaries believe the information in this document is accurate as of its publication date. The information is subject to change without notice.