

Colruyt ensures data privacy with Identity & Access Management.

Table of Contents

Executive Summary

SECTION 1: CHALLENGE **2**

Safeguarding the privacy of personal data

Reducing the security risks of IT automation

Securing a new distributed environment

SECTION 2: OPPORTUNITY **3**

Preventing unauthorised access to systems

Securing the perimeter

Audit trails for easier compliance

SECTION 3: BENEFITS **5**

Improved data security reduces risk

SECTION 4: CONCLUSIONS **6**

ABOUT CA

Back Cover

Executive Summary

Challenge

With all its processes — from point of sale transactions to logistics management — reliant upon IT, retailer Colruyt needs to ensure its systems and data are secure. In particular, the company needs to lock down access to servers that support its email and HR systems. Any unauthorized access to confidential data could result in a breach of European privacy laws and expose the company — and its staff — to external security risks. When Colruyt migrated its HR and email systems from a mainframe to a distributed environment, maintaining high levels of data security was paramount.

Opportunity

Colruyt uses a CA Identity & Access Management solution to prevent unauthorised access to its HR and communications systems and data. Using the solution's Policy Management Database and Web-based graphical user interface, Colruyt can specify complex access rights for its IT department across both Microsoft and Linux platforms. In addition to safeguarding access, the CA solution also provides comprehensive audit trails for regulatory compliance purposes. The implementation has been such a success that Colruyt is now extending the CA solution to other production systems.

Benefits

Colruyt can balance data security with the IT department's need to access core systems. As a result, it has been able to:

REDUCE RISK Colruyt's systems are protected from malicious threats that could impact business continuity

ENSURE COMPLIANCE WITH PRIVACY LAWS Employees' records are protected against unauthorised access.

This helps to safeguard the reputation of the company, which will be key as it continues to grow its operations.

“Mitigating the risks of a security breach and the potential impact on the business is essential.”

Hein Coulier
Security Officer, Colruyt

Safeguarding the privacy of personal data

The security of personal data is a key concern for European businesses. With news reports frequently covering the loss of confidential personal data by both government and commercial organisations, data protection is a subject matter that rarely leaves the headlines.

European privacy laws are well established, dating back to the European Commission’s adoption of the Data Privacy Directive in 1995. This level of maturity has not, however, prevented a recent series of highly-publicised breaches of privacy and data protection laws.

With identity theft on the increase, the agencies responsible for enforcing these privacy laws are more rigorous than ever, and European businesses are all too aware of the devastating reputational and financial impact of inadequate security policies.

Even if a company operates in the business-to-business space, data protection is still a concern — and may even be subject to formal non-disclosure and confidentiality agreements. All companies also hold a certain amount of human resources (HR) data on their employees, which must be adequately protected to comply with privacy laws.

Compliance, however, is not the only driver for securing IT systems. Organisations also need to protect themselves against malicious intrusion attempts that could not only threaten data integrity but also cause IT downtime and impact business continuity.

Reducing the security risks of IT automation

Belgian retailer Colruyt holds data on more than 20,000 employees as well as some customer related information. One of Belgium’s largest commercial companies, Colruyt sells groceries, toys and baby goods through brands such as Dreamland, Dreambaby, Coccinelle France and OKay as well as Colruyt. The company also supplies independent shopkeepers through its wholesale and distribution business, which includes 16 cash and carry stores in North East France.

Colruyt’s business strategy is based on offering consumers the lowest prices for its goods. For this strategy to succeed Colruyt needs to maintain very low operating costs, so the majority of its business processes rely at least to some degree on automated systems. This increasing dependency on IT has brought with it a growing awareness of security issues and the potential impact of a system breach.

In 2005, Colruyt initiated a project to improve the security of its production data. Hein Coulier, Security Officer at Colruyt, comments, “All our business functions rely on IT. From point of sales systems and logistics applications to HR and finance — an IT outage could have a massive impact on the productivity and profitability of the business. As a result, mitigating the risks of a security breach and the potential impact on the business is essential.”

Securing a new distributed environment

The company’s existing mainframe environment was extremely secure with system access governed by a CA mainframe Identity & Access Management solution. With the number of applications being developed and used by the business growing, Colruyt had made the decision

to move some of its core systems to a distributed environment. This would enable it to deploy new systems more quickly, thus increasing business agility.

Maintaining the security of its systems throughout this transformation was critical. “The new distributed IT infrastructure did not offer as much inbuilt security as our mainframe platform. We were therefore eager to implement an extra layer of security to protect sensitive data and our core systems,” comments Coulier.

This need was reinforced when Colruyt’s IT department, Colruyt Group Services, conducted a comprehensive risk assessment of the security threat to the distributed environment. With 900 IT staff including up to 600 software engineers, Colruyt needed an efficient way to manage user access accounts that would enable it to meet its stringent security policies.

SECTION 2: OPPORTUNITY

Preventing unauthorised access to systems

After investigating a number of solutions available on the market, Colruyt selected a CA Identity & Access Management solution to help it enforce its security policies in the new distributed IT environment. CA Access Control offered the fine-grained controls required to achieve this, as well as simple centralised management.

“As we were already using the equivalent CA Identity & Access solution for our mainframe systems, we already had a good grasp of how the solution would work,” comments Coulier. “Minimising the risk involved in the implementation was high on the agenda, and the CA solution offered a good low-risk choice.”

CA Access Control r12 was deployed to protect Colruyt’s HR systems as part of CA’s BETA programme in January 2008. The implementation was extended to include its communications infrastructure in April 2008, which supports 3,800 users — by January 2009, this number will rise to 20,000.

CA Access Control is used in production, development and test environments. Due to the company’s server consolidation efforts, this amounts to just four production servers (on a total of 14) running Microsoft and Linux operating systems.

Securing the perimeter

CA Access Control provides a solid wall to prevent certain users accessing data and systems specified by Colruyt. Using the solution’s Policy Model Database, Colruyt is able to manage permissions and regulate access to resources, programs and data via a central online graphical user interface. These are categorised by department and role for simple management. For example, developers working on HR applications are able to access HR data, however developers working on finance applications cannot.

The solution is currently used to manage access rights for more than 200 members of the IT department using more than 24 different policies. The volume of both users and policies will increase as Colruyt extends its use of the CA solution to all its core production systems, which will eventually encompass more than seven production servers (on a total of 20).

“CA Access Control provides a solid wall to prevent certain users accessing data and systems specified by Colruyt.”

Hein Coulier
Security Officer, Colruyt

Although access policies can be complex and involve many variables, they are easily managed via the solution's policy management interface. Adding and updating policies, or adding new users, is also quick and straightforward as the solution's policy definitions are role-based and can be deployed automatically.

Audit trails for easier compliance

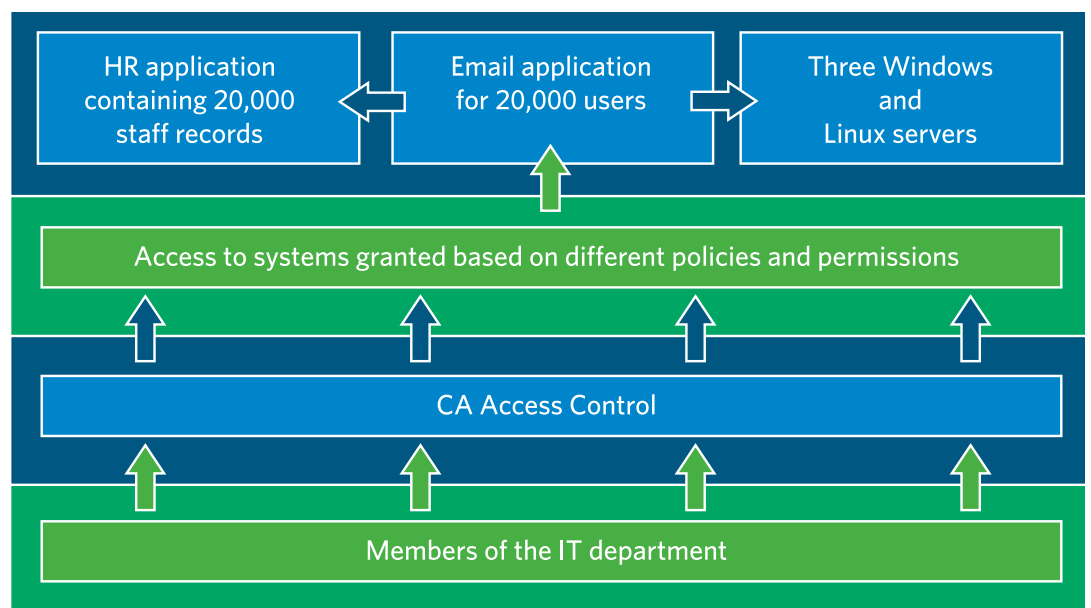
In addition to preventing unauthorised access to sensitive data, CA Access Control provides Colruyt with comprehensive audit trails of all access to HR and communications systems.

The solution can even automatically provide tailored reports for demonstrating compliance with specific legislation, such as the Sarbanes-Oxley Act, or ISO standards accreditation.

POLICY-BASED ACCESS MANAGEMENT FOR INCREASED SECURITY

Using CA Access Control, Colruyt can limit access to HR and email applications and data according to user roles.

FIGURE A



“The CA Identity & Access Management solution provides a cost-effective foundation for our internal security policies. It is easy to manage, and its fine-grained controls enable us to achieve the correct balance between privacy and providing necessary access to systems.”

Hein Coulier
Security Officer, Colruyt

Improved data security reduces risk

Using CA Access Control, Colruyt is able to safeguard sensitive data while minimising the IT management overhead.

“The CA Identity & Access Management solution provides a cost-effective foundation for our internal security policies,” comments Coulier. “It is easy to manage, and its fine-grained controls enable us to achieve the correct balance between privacy and providing necessary access to systems.”

By enhancing its Identity & Access Management capabilities on core systems, Colruyt is able to:

SAFEGUARD BUSINESS CONTINUITY AND REDUCE RISK Colruyt can protect its HR and email systems from malicious sabotage, which could impact availability and therefore business continuity.

SIMPLIFY COMPLIANCE WITH DATA PRIVACY LEGISLATION CA Access Control prevents unauthorised access to core data and systems in line with European privacy laws.

PROTECT COMPANY REPUTATION Colruyt’s 20,000 employees know that their personal data, such as home address, email address and salary, are protected from unauthorised access and possible identity theft. Shareholders can also rest assured that the company is compliant and operating within accepted risk parameters.

In addition to current privacy legislation, Colruyt is fully aware that regulations are constantly changing, and that rules governing access to financial systems could soon become a reality for businesses operating outside of the US.

“CA Access Control has given us a head-start for complying with any legislation that mirrors the Sarbanes-Oxley Act,” adds Coulier.

The company also has a head-start for securing other systems via the CA solution. CA Access Control is highly scalable, which will be key as the company continues to grow its business and establish greater levels of IT automation.

SECTION 4: CONCLUSIONS

Compliance, customer service levels and a company's reputation can all be impacted by poor data protection.

To ensure that systems are protected against unauthorized access, organisations need to establish an effective Identity & Access Management strategy. This is particular key when safeguarding access to core production systems and raw data, which could be used for identify theft.

Using an automated Identity & Access Management solution with policy-driven security management, organisations can easily administer a plethora of user accounts with varying access privileges. This will not only help to protect data but also safeguard compliance and business continuity.

To learn more about the CA Identity & Access Management architecture and technical approach, visit www.ca.com/us/identity-access-management.aspx.

CA, one of the world's largest information technology (IT) management software companies, unifies and simplifies the management of enterprise-wide IT for greater business results. Our vision, tools and expertise help customers manage risk, improve service, manage costs and align their IT investments with their business needs.

Learn more about how CA can help you transform your business at [ca.com](https://www.ca.com)

