



Ensuring Identity Security with Omada

Customer Stories: Achieving Stronger Security Through Identity Governance



Introduction

Modernizing Identity Security: Real Customer Outcomes

For many organizations, identity security remains a significant vulnerability. Legacy access management approaches often lack visibility into who has access to what, creating blind spots that increase risk. Manual access reviews, inconsistent policy enforcement, and fragmented systems make it difficult to prevent unauthorized access or respond quickly to threats.

Moving to a modern Identity Governance and Administration (IGA) solution can transform this challenge. This eBook shares how leading organizations across industries are achieving measurable security improvements by modernizing their identity governance with Omada. From automated policy enforcement to continuous compliance visibility, these real-world stories demonstrate what is possible when identity security is proactive, not reactive.

If your team is ready to reduce risk, strengthen access controls, and gain visibility across your identity landscape, these customer experiences can guide your path forward.



Table of Contents

This eBook features organizations that turned identity governance into a proactive security advantage. See how they achieved measurable improvements – from 50%+ risk reduction to eliminating hundreds of orphaned accounts – by implementing modern IGA with Omada.

BankData

Bankdata Streamlines Identity Governance with Omada Identity Cloud

Bankdata, a leading IT service provider for financial institutions in Denmark, recognized the potential to enhance its identity governance and administration (IGA) capabilities with a cloud-based solution. As a long-time customer of Omada's on-premises IGA solution, Bankdata was already familiar with the value of Omada's technology. However, they sought to leverage the scalability, efficiency, and automation benefits offered by a cloud-based approach.

Requirements and Selecting Omada Identity Cloud

By adopting a move-to-cloud strategy and transitioning to [Omada Identity Cloud](#), Bankdata aimed to streamline operations and improve efficiency. They also sought to improve scalability to ensure that their IGA solution could easily adapt to changing organizational needs. Additionally, Bankdata wanted to enhance security by benefiting from Omada's cloud-based security measures and compliance capabilities.

Omada Identity Cloud provided Bankdata with a comprehensive solution that met their specific needs, including a unified access management platform, automated join, move, and leave processes, and seamless integration with both on-premises and cloud applications.

[The Omada Identity Cloud Accelerator Package](#) further accelerated Bankdata's migration, allowing them to implement the solution within 12 weeks. This pre-built toolkit provided standardized deployment, best-practice process design, and user training. Leveraging the Accelerator Package and their existing familiarity with Omada, Bankdata was able to achieve a rapid return on investment.

Deployment, Key Benefits and Results

Bankdata was very impressed with the speed of implementation and was able to onboard their HR system, their primary Active Directory (AD) instance, and Entra ID to Omada Identity Cloud in less than three months. Bankdata has experienced several key benefits since deploying Omada Identity Cloud. The solution has enhanced [security](#) and [compliance](#) by offering even more robust controls and automated reporting, while also improving [efficiency](#) through automation of manual tasks.

Results

Bankdata has achieved significant improvements in its identity and access management capabilities since deploying Omada Identity Cloud. By leveraging the solution's advanced features and automation capabilities, Bankdata has been able to enhance security, improve efficiency, and shift focus from operational to business-oriented activities benefiting the organization as a whole. With Omada, Bankdata has achieved significant improvements in productivity and efficiencies through:

- ✓ Automatically assigning **more than 60%** of access rights through Omada's roles and policies
- ✓ Automating the entire Identity Lifecycle Management (ILM) process, freeing up the IAM team to focus on more strategic initiatives like onboarding applications and systems
- ✓ Ensuring least privilege by automatically removing unnecessary access when an employee moves teams



Country: Denmark

Industry: Financial Services

Solution: Omada Identity Cloud

Key Takeaways

- **Rapid implementation:** Fully onboarded HR system, Active Directory, and Entra ID in under 3 months, demonstrating fast time-to-value
- **60% automation of access assignments:** Omada's roles and policies automatically grant the majority of access rights, eliminating manual provisioning bottlenecks
- **IAM team capacity shift:** Full Identity Lifecycle Management automation freed the IAM team from operational tasks to focus on strategic initiatives like application onboarding
- **Continuous least privilege enforcement:** Automatic removal of unnecessary access when employees change roles prevents privilege creep and reduces security risk
- **Enhanced compliance posture:** Robust automated controls and reporting strengthen security governance while reducing audit preparation effort

[Read the full Story](#)

Commerz Real

Commerz Real AG Chooses Omada Identity

Commerz Real AG is a wholly owned subsidiary of the major German banking and service provider, Commerzbank AG. To further strengthen its security and maintain a consistent compliance level, Commerz Real implemented a central role-based identity management solution with single sign-on.

Omada's all-in-one solution for automated role-based access control, [provisioning](#), [identity lifecycle management](#), and compliance control proved to be an ideal match for their solution requirements. A key deciding factor for selecting Omada Identity Cloud was the easy configuration and best-practice standard processes that provide built-in advanced IAM features:

- ✓ Self-service access request portal for improved user experience
- ✓ Automated attestation workflows eliminate simple repetitive tasks for both business users and the IT-department
- ✓ Compliance dashboards for on-demand access intelligence overview and reporting
Increased IT security via automated segregation of duties policy validation

"Omada's solution is easy to use and has transformed previous resource-intensive repetitive tasks into centrally controlled automated processes. Additionally, the automated onboarding and management of applications and identities according to regulations and policies, means

that compliance is automatically implicit – so for us identity management is cool." – Christian Ebert, IAM Project Manager at Commerz Real AG.

Identity Lifecycle Management

Omada Identity provides all necessary processes for full automation of tasks related to [identity lifecycle management](#). A self-service portal enables users to request access to resources, while managers and role owners can revoke access that is no longer needed. Processes for role-based access control grant appropriate access rights to employees based on job functions. At the same time, Omada Identity ensures that no critical access rights combinations are assigned.

In addition to identity lifecycle workflows, the solution automates the processes for periodic reviews and quality assurance of roles and permissions. Automated attestation workflows generate audit-ready reports, enabling compliance with complex regulatory requirements.

"The business benefits of identity management are obvious. In a strictly regulated industry like ours, compliant and secure access is essential. Omada's solution has provided Commerz Real with a proactive approach, so we continuously have a clear overview of the actual state of our access governance." – Christian Ebert, IAM Project Manager at Commerz Real AG.



Country: Germany

Industry: Finance

Solution: Omada Identity Cloud

Key Takeaways

- **Automated transformation:** Resource-intensive manual tasks replaced with centrally controlled automated processes across the entire identity lifecycle
- **Compliance by design:** Automated identity management according to regulations makes compliance "automatically implicit" - built-in, not bolted-on
- **Intelligent access control:** Self-service portal combined with role-based access and segregation of duties (SoD) prevents toxic access combinations while empowering users
- **Continuous audit readiness:** Automated attestation workflows and periodic reviews generate audit-ready reports for complex regulatory requirements
- **Proactive governance visibility:** Real-time oversight of access governance state enables continuous monitoring vs. reactive, point-in-time approaches which are critical for regulated industries

[Read the full Story](#)

DEKRA

Moving From a Home-Grown to a Modern IGA SaaS Solution in Record Time

As part of their digital transformation, DEKRA moved from an in-house developed access management solution to a modern, cloud-based [Identity Governance and Administration \(IGA\) solution from Omada](#), which has led to significant productivity improvements, as well as substantial cost savings.

Business Drivers

DEKRA's digital transformation permeated the entire organization, geared towards driving rapid growth in all areas. However, with growth came changes in business and cybersecurity requirements, as well as the need to keep the entire workforce productive and efficient. To keep up with these changes, DEKRA needed a modern IGA solution to manage access to all internal resources without compromising the efficiency of administrators and business users.

Requirements and Selecting Omada

When evaluating both their needs and wants, DEKRA knew they not only needed a standards-based IGA tool that was not overly complex to manage but also that would be able to support a variety of governance tasks to enable their digital transformation. Omada Identity Cloud, a SaaS-based IGA solution, jumped to the top of the list, as it satisfied nearly 100% of DEKRA's requirements. Omada was also able to fulfill DEKRA's requirement to integrate with a wide range of

applications to support employees and contract workers across multiple countries and regions.

Implementation and Use Case

The Omada setup took a week, and the implementation was rolled out successfully in four phases, leveraging the framework outlined in Omada IdentityPROCESS+. DEKRA has since deployed the following use cases for Identity Governance and Administration: [Identity lifecycle management](#), access request and approval process, recertification, automation of audit process.

With Omada Identity Cloud, DEKRA can now provision the right identities to have access to the right applications for the right reasons. It has also made it easier to assign access across regions and manage the end-to-end lifecycle of each identity as roles and responsibilities change. Plans to integrate with SuccessFactors and ServiceNow are underway.

Results

They have been able to streamline and automate the access request and approval process, reducing the number of calls to the Help Desk, as well as ensuring quicker access where appropriate, with the proper security controls in place. DEKRA has seen tangible returns on investment (ROI) within 6 months and is quickly scaling the solution to meet additional use cases.



Country: Germany

Industry: Public Safety

Solution: Omada Identity Cloud

Key Takeaways

- **Achieved foundational IGA governance:** Right identities accessing right applications for right reasons with proper security controls
- **Operational efficiency gains:** Streamlined access request/approval process reduced Help Desk call volume and accelerated provisioning times
- **Rapid ROI achievement:** Tangible returns realized within 6 months of implementation
- **Multi-region scalability:** Simplified access management across geographic locations with centralized governance
- **Lifecycle automation:** End-to-end identity management adapts automatically as roles and responsibilities evolve
- **Strategic expansion underway:** Scaling to additional use cases with planned SuccessFactors (HR) and ServiceNow (ITSM) integrations

[Read the full Story](#)

Bayerische Landesbank (Bayern LB)

Bayerische Landesbank (Bayern LB) Looked to Omada to Deploy a Modern, Standards-Driven IGA Solution

Bayern LB has over 7000 personal and technical identities that they need to manage, secure and enable. As part of their identity security journey, Bayern LB needed a centralized identity governance and management platform to meet compliance mandates, reduce risk while further enabling their entire workforce. They looked to Omada to deploy a modern, standards-driven [identity governance and administration \(IGA\) solution](#).

Requirements and Selecting Omada

Bayern LB chose Omada due to our proven ability and experience in deploying Identity Governance controls to help organizations meet audit demands, while maximizing business efficiencies. It was important for Bayern LB to work with an IGA vendor that had supported other companies with similar requirements and challenges in their region. When evaluating their technological requirements, Omada inevitably scored the highest in functionality and ability to execute, with our high flexibility in adapting the solution to meet the expectations of auditors, while keeping the deployment standards-driven for future scale.

Use Case and Environment

Having a single, centralized solution to manage and control all of Bayern LB's identities was critical. As such, Omada Identity was chosen because of its ability to be the single source of truth for identity governance and access administration. Bayern LB leverages Omada for the following use cases:

1. [Identity Lifecycle](#)
2. Access Control and Requests
3. Segregation of Duties
4. Reconciliation
5. Recertification Reporting

Omada Identity provides Bayern LB with end-to-end [identity lifecycle management](#) for all the bank's identities. Bayern LB uses Omada to leverage standard workflows and processes for policy-based access management and governance which is customized per their unique business requirements. They also integrated Omada with their Active Directory environment to provision and de-provision access to in-house applications, legacy mainframe applications as well as to 3rd party applications.

Results

Since deploying Omada Identity, Bayern LB has seen marked improvements within a year in the following areas:

- ✓ Greater than 50% reduction in risk through access governance and better visibility
- ✓ Improved security and optimized operations through implementation of SoD
- ✓ Improved efficiency through automated workflow-based access management requests and approvals
- ✓ Higher transparency through recertification of identities and associated permissions.



Country: Germany

Industry: Banking

Solution: Omada Identity

Key Takeaways

- **50%+ risk reduction achieved:** Access governance and comprehensive visibility into identity landscape reduced organizational risk by more than half within the first year
- **Single source of truth established:** Centralized IGA platform replaced fragmented systems, enabling end-to-end lifecycle control across all bank identities
- **Complex integration scope:** Seamlessly connected Active Directory, legacy mainframe systems, in-house applications, and third-party systems for consistent access management across diverse infrastructure
- **Workflow automation and transparency:** End-to-end identity lifecycle management for all of Bayern LB's identities
- **Segregation of Duties implementation:** SoD controls improved security and optimized operations across the organization

[Read the full Story](#)

Coca-Cola Hellenic Bottling Company

World's Third Largest Bottler of Coca-Cola Optimizes Identity Management with Omada

Coca-Cola Hellenic Bottling Company (CCHBC), the world's third-largest bottler of Coca-Cola, faced challenges managing access for its 40,000 employees across 29 countries. Their legacy SAP-based solution struggled to keep up with frequent user access changes, impacting productivity.

The Need for Modern IGA

In a quest to overcome the limitations of their legacy SAP-based system, Coca-Cola Hellenic Bottling Company (CCHBC) transitioned to Omada Identity in 2020. CCHBC's outdated solution struggled to keep pace with their dynamic access needs, leading to provisioning inefficiencies and continuous disruptions. Omada Identity, with its modern, secure, and flexible approach, offered a powerful alternative to manage the entire identity lifecycle for CCHBC's vast workforce and technical accounts within Microsoft Active Directory.

Key Improvements After Omada Identity

- ✓ **Automated Processes:** Omada automated provisioning tasks, eliminating manual processes and reducing provisioning times by 80%. In one instance, Omada automated the assignment of over 1 million tasks within a week, a feat impossible with manual efforts.
- ✓ **Improved Efficiency:** Streamlined workflows and self-service capabilities empowered users and reduced help desk tickets.

- ✓ **Enhanced Security:** Omada enforced strong security policies and provided complete visibility into CCHBC's identity landscape, enabling proactive risk management.
- ✓ **Global Reach:** Omada seamlessly integrated with business-critical apps and systems including SAP HCM, Active Directory, Azure AD, ServiceNow, and over 220 offline systems, ensuring consistent access management across a vast infrastructure.

Impact on Business

- ✓ **Simplified Access Management:** Omada provided a central platform for requesting and granting access to business resources, simplifying processes, and improving information distribution across systems.
- ✓ **Reduced Disruptions:** Omada's automatic provisioning ensured that users have uninterrupted access, significantly improving overall business continuity.
- ✓ **Collaboration and Expertise:** The close collaboration between CCHBC and the Omada team has been instrumental in achieving success. Omada's IGA expertise ensured CCHBC leveraged best practices and avoided unnecessary configurations.

CCHBC is proud of the IGA project's rapid implementation, achieved within six months, highlighting the efficiency of Omada's methodology.



Country: Switzerland

Industry: Consumer Products

Solution: Omada Identity

Key Takeaways

- **Exceptional automation scale:** Automated 1 million access assignment tasks within one week, achieving what would be impossible manually while reducing provisioning times by 80%
- **Enterprise-wide integration:** Seamlessly connected 220+ offline systems plus business-critical applications (SAP HCM, Active Directory, Azure AD, ServiceNow) for consistent access governance across massive infrastructure
- **Enhanced security posture and visibility:** Complete visibility into the identity landscape enabled proactive risk management through enforced security policies and centralized access control
- **Operational efficiency gains:** Streamlined workflows and self-service capabilities reduced help desk ticket volume while empowering users to request and receive access faster
- **Business continuity improvement:** Automatic provisioning eliminated access disruptions, ensuring users maintain uninterrupted access to critical resources during role changes

[Read the full Story](#)

From Risk to Control

Telenor Norway

Norway's Number One Telecommunications Provider Chooses Omada for Identity and Access Governance

Telenor was looking for a modern in-house solution for Identity Governance and Access Management (IGA) to improve their day-to-day operations across the organization, enhance their security posture, and meet various compliance mandates.

Business Drivers and Requirements

Telenor has been modernizing their business and working towards automating processes to free up resources wherever they can. The organization is split up into various business units across multiple geographies, which over time created data silos and a lack of transparency, which became a primary driver for them seeking out a modern approach to how they manage, secure, and enable their workforce. Having centralized solutions that were able to be counted as a single source of truth, providing insights throughout the organization was critical.

Use Cases

Telenor chose Omada to support them with their business requirements for security improvement, risk mitigation, and compliance by looking to a standards-driven approach to IGA so as to avoid over-customization. They looked to [Omada Identity Cloud](#) primarily to aid in the following initiatives:

- ✓ Automating user management by enabling seamless workflows for access requests and reviews
- ✓ Minimizing the number of orphaned accounts that had no ownership
- ✓ Integrating a wide variety of applications and systems
- ✓ Managing the identity lifecycle to ensure proper access for all identities on day one of a role, and removing access when it is no longer required
- ✓ Improving policy and role management to ensure that policies and roles are consistently right-sized to meet the needs of the business
- ✓ Complying with audit and compliance mandates with easy access to overviews, reports, and dashboards

Results and Improvements

Since implementing Omada, Telenor has been able to eliminate hundreds of orphaned accounts, gain complete visibility into who had access to what, enable employees or contractors to now easily request and get access to devices and applications quicker, and better prepare for audits.

As a result of their deployment of Omada Identity, Telenor was able to minimize tedious tasks for business users and administrators, improve their security posture by eliminating orphaned accounts, and be better prepared and positioned to meet the continually changing demands of compliance mandates.



Country: Norway

Industry: Telecommunication

Solution: Omada Identity Cloud

Key Takeaways

- **Eliminated hundreds of orphaned accounts:** Comprehensive visibility revealed and removed accounts with no ownership, significantly reducing security risk and attack surface
- **Broke down organizational data silos:** Centralized platform unified identity management across business units and geographies, providing single source of truth
- **Accelerated access provisioning:** Automated workflows enabled employees and contractors to request and receive device and application access faster, improving productivity
- **Lifecycle automation from day one:** Ensures appropriate access on first day of employment and automatic removal when no longer required
- **Audit readiness and compliance positioning:** Reports and dashboards better prepared the organization to meet changing compliance mandates while minimizing administrative burden

[Read the full Story](#)

Conclusion

Security, Strengthened.

The organizations featured in this eBook faced a common challenge: identity security gaps that created risk, limited visibility, and kept security teams in reactive mode. Through Omada, they transformed identity governance from a vulnerability into a strategic control. The results are concrete: automated policy enforcement replaced manual reviews, continuous visibility eliminated blind spots, and proactive access controls reduced unauthorized access risks. These are not just security improvements – they are measurable gains in risk reduction, compliance confidence, and operational resilience.

Modern identity threats demand modern defenses. With Omada, identity security becomes continuous, intelligent, and fully integrated across your enterprise. From access intelligence to automated lifecycle management, these customer stories demonstrate what is possible when governance is built into every identity decision. If your organization is ready to move from reactive risk management to proactive identity security, Omada can help you get there.

Ready to strengthen your identity security posture? [Schedule a demo](#) today to see how Omada can help you reduce risk, gain visibility, and build a foundation for continuous security.





Omada simplifies Identity Governance by providing a full-featured, cloud-native IGA solution that streamlines the complex processes of managing user identities, access, and entitlements. With a focus on automation and user-centric design, Omada reduces manual tasks and enhances operational efficiency, ensuring that organizations can easily enforce security policies, comply with regulations, and manage user access at scale. By leveraging advanced technologies such as AI-driven decision-making and role-based access control (RBAC), Omada enables businesses to achieve stronger security, better compliance, and improved user experiences—without the complexities traditionally associated with identity governance.