

Telecommunications

CASE STUDY

How identity based access & connectivity is enabling Vodafone's remarkable digital transformation and growth since 20 years

HOW VODAFONE GROUP AND VODAFONE GERMANY FORTIFIED AND CENTRALIZED ALL THIRD PARTY AND VENDOR REMOTE ACCESSSES

Vodafone GmbH is a German subsidiary of the British telecommunications company Vodafone Group. It offers mobile communications, DSL, cable internet, fixed-line telephony, cable TV and IPTV in Germany. With over 67.5 million switched SIM cards in Q2 2022, Vodafone is one of the largest mobile providers in Germany in terms of subscriber numbers.

Vodafone set out to improve their overall security posture and provide a seamless user experience for internal and third-party user access of the company's applications. Over the years, back from 2003, Vodafone Group extended its services to several European countries and from the beginning sought to offering a series of diverse telecommunication services. Vodafone Group was looking for a security model that would support their growth and business strategy objectives, as well as to more efficiently organize the corporate network with all subsidiaries and secure it with regard to high compliance requirements, e.g. in accordance with KRITIS and NIS guidelines.

The company's Information Security Team who led the shift to a new security strategy was aware that Vodafone's existing IT infrastructure limited flexibility and lacked identity-based authentication. They knew the company's growing attack surface was leading to even greater risk but also had to prioritize business agility and security with pursuit of further tethering and expansion. Vodafone's centric and specialized approach to providing telco services made operational agility and efficiency top priorities, with zero trade-off on organizational and data security.

Reducing their security risks by minimizing their attack surface and meeting the ever-changing compliance requirements to provide secure remote access, particularly in the verticals, were critical in continuing to scale up. The company was looking for a solution to centralize identity-based remote user access to mission-critical applications and resources, with a range of challenges they set out to overcome.

THE EXISTING TECH STACK & THE CHALLENGES TO OVERCOME

With Vodafones global departments, internal users and third party vendors located across Europe, it was essential to blend speed and agility with improved secure connectivity to support the business and maintain productivity. Users, working both internally and remotely, were connecting to private circuits through firewalls in internet breakout locations. Key business applications were accessed via VPN and virtual desktops, increasing the attack surface and adding further complexity, latency and overhead to the infrastructure.

When starting their new journey to connectivity and secure user access, Vodafone used VDI as a security and performance tool, alongside MFA, SSO and MDM, with all devices joined to a nested domain. Keeping all applications protected with MFA was critical to Vodafone, and while MFA was able to provide this for some applications, others posed challenges for MFA integration because of their age, provenance or architecture.

One critical example was one billing application, which would have otherwise required additional coding and customization to apply MFA to it. With the sensitive data and daily workflows involved using this application, finding a way to authenticate users and secure user access and connectivity with MFA was critical. Fronting connections with VISULOX did the trick. Simple.

Vodafone was eager to adopt and implement a security model that would support peak performance and efficiency, while meeting the telco industry's demanding compliance requirements with full control and ownership of sensitive content and data.

Outcomes



LEVERAGING IT-SECURITY MEASURES

Reduced organizational attack surface and improved security posture



MEETING AUDIT TARGETS

Maximized and optimized operational agility and efficiency while staying compliant



RETURN ON SECURITY INVEST

Over \$500,000 in annual cost-savings



ONE USER - ONE IDENTITY

Elimination of functional accounts and clear assignment of user identities



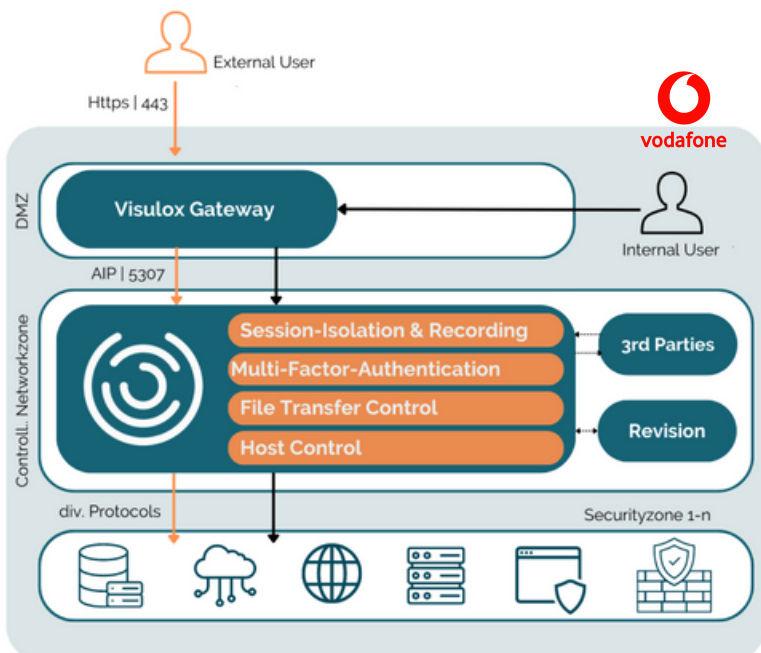
Every day, well over 2,500 external employees from various partners and service providers work remotely, directly or indirectly, on the systems in the internal IT and OT infrastructure. 2,500 users that we provide single access via our VISULOX Remote PAM cluster. amitego helps us to further develop our own features on a daily basis and ensures smooth, highly available access to the Vodafone infrastructure.

Group Information Security Team
Vodafone

NEXT STEPS: REPLACING THE VPN TO IMPROVE SECURITY, PERFORMANCE & PRODUCTIVITY WHILE SCALING UP

The team was ready to remove their virtual desktops and simplify their infrastructure, while simultaneously implementing a zero-trust access framework that would allow them to review WAN (Wide Area Networking) strategy in the future while replacing VPNs today. Under the leadership of Vodafone's CISO, the organization was ready to make the shift and adopt VISULOX identity-based access solution, proactively taking cost-effective measures to further secure the organization and underpin performance.

THE VISULOX SOLUTION



Goals

1

AGENTLESS DEPLOYMENT

Easily, quickly and cost-effectively deploy and implement a single secure access and connectivity solution at minimal overhead and to lay a zero-trust foundation and meet industry compliance requirements.

2

SEAMLESS INTEGRATION

Fill in MFA and SSO gaps, further increasing the value and extending use of existing solutions for MFA, SSO, and MDM.

3

MODERN USER EXPERIENCE

Improve security posture while maintaining optimal performance and user experience for internal and remote users.

4

CENTRALIZATION OF ALL ACCESS

Replace VPN used for remote vendor access to key business applications within the cross-county multi tenant organizational infrastructure.

5

LOWERING ADMINISTRATION EFFORT

Move away from reliance on domain-joined device to support BYOD and improve business agility.

WHY VODAFONE CHOSE VISULOX: SECURE ACCESS AND UNMATCHED USER EXPERIENCE WHILE STAYING COMPLIANT

In evaluating the solutions on the market and ultimately choosing VISULOX, Vodafone felt they gained the fastest and most secure access solution available. Key to their decision were the facts that VISULOX has no access to their data, stores nothing in the cloud, and provides speedy, low-latency delivered service. The telco industry's compliance requirements are increasingly rigid and demanding, particularly adherence to privacy policies related to security and storage of sensitive data, like GDPR standards. VISULOX scalable architecture empowers Vodafone to fully own and control all critical content and data.

NEW SECURITY MEASURES IMPLEMENTED COST-EFFECTIVELY AND WITH EASE

VISULOX was initially deployed for Vodafone within just two days providing a nearly instantaneous improvement to business agility and operational efficiency for an organization with over 2.500 concurrent remote, internal and third-party users - and growing at a rapid pace. With the new cost-effective identity-based access strategy as a foundation.

Vodafone's subsidiaries could be easily added to their central IT systems and applications within minutes. Key stakeholders and users gained just-in-time secure access and connectivity with minimal management overhead.

RESULTS



Reduced attack surface, improved security posture with minimal management overhead and automated workflows to relieve IT-department



Unmatched speed and ease of deployment and implementation taking just two days to get up and running with immediate results



Built foundation for a zero-trust framework and secure remote user access and connectivity to be future proof and operational costs sensitive

ABOUT amitego

Too many critical assets and systems remain exposed because traditional secure access solutions are not able to protect the high-risk access scenarios and legacy applications that keep modern business operations running. VISULOX provides the only trustless zero-trust access solution, giving organizations visibility and access control over the users who leave them most exposed to risk, including third-party workers and remote OT operators.

IT SECURITY. MADE IN GERMANY SINCE 2003.

Request a demo with us
to learn more:

[Request demo](#) 



"Working with the amitego team continues to prove that identity-based access based on a trust-less architecture will bring our security posture and user experience to the next level"

amitego