Guardicore

Case Study

*"Guardicore helped us to implement tight network segmentation across on-premises and cloud environments. With Guardicore we are effectively protecting our critical assets and applications."*

Vice President, Information Security at Large European Bank

INDUSTRY

Financial Services

MAIN USE CASES

- Reduce Compliance Costs
- Environments Segmentation
- Secure Cloud and Container Environments
- Security Processes Automation

FEATURES USED

- Visibility
- Application Dependency Mapping
- Auto-generated Segmentation Policies
- DevOps Policy Automation
- Change-management Integration

# Large European Bank Selects Guardicore to Reduce Security and Compliance Costs with Innovative Approach to Segmentation

## The Customer

### A Large European Bank

A multinational investment and financial services company, providing services to customers across more than 50 countries in Europe, North America, and Asia, needed to improve its compliance posture. Facing cybersecurity regulations from multiple authorities in Singapore, UK, US, and Europe, the organization's main goal was to achieve workload segmentation and separation of the environments in its data center.

## The Challenge

### Meeting Security and Compliance Requirements with Segmentation

The increased focus from regulators on tightening data center security and ensuring financial services market stability resulted in new regulations that required the bank to meet technical requirements through segmentation.

Internal auditors had also alerted the organization to the security risks posed by flat networks, that will amplify the impact of a security breach. A major concern was an internal threat scenario where human error or unauthorized activity would lead to an information leak or production error, potentially destabilizing the bank's entire environment.

To address these challenges, the bank began implementing internal data center network segmentation.

## Selecting a Solution
### A Struggle with Legacy Firewall Complexity

The initial segmentation effort was done with traditional tools such as Firewall rules and VLANs. This project was taking significant time, requiring multiple stakeholders and teams' attention, causing production downtimes and policy ambiguities. As a result, the bank was paying significant fines for non-compliance, in addition to high implementation costs.

With the cost of traditional approaches being unviable, the bank's IT team started to look into alternative and more cost effective segmentation solutions to meet the compliance requirements. In addition to the on-premises segmentation, the bank was also looking for a cloud and container-ready solution.

When the evaluation team came across the Guardicore Centra Security Platform, they were intrigued by the level of visibility and policy flexibility it demonstrated during the proof of concept. Additionally, the DevOps integration and automation impressed them. These capabilities simplified policy creation and enforcement in a unified manner across multiple infrastructures. But most importantly, the Guardicore team showed full commitment to success throughout the POC and after. This true partnership attitude distinguished Guardicore's value even further.

After a thorough evaluation process that included multiple vendors, the decision-makers in the bank's infrastructure and IT security teams came to a consensus: Guardicore's technology offered the simplest, most straightforward path to micro-segmentation. Centra also aligned with the bank's future strategy. It would give the organization both granular visibility into the East-West traffic and the ability to enforce segmentation policies in its new multi-cloud and container environments.

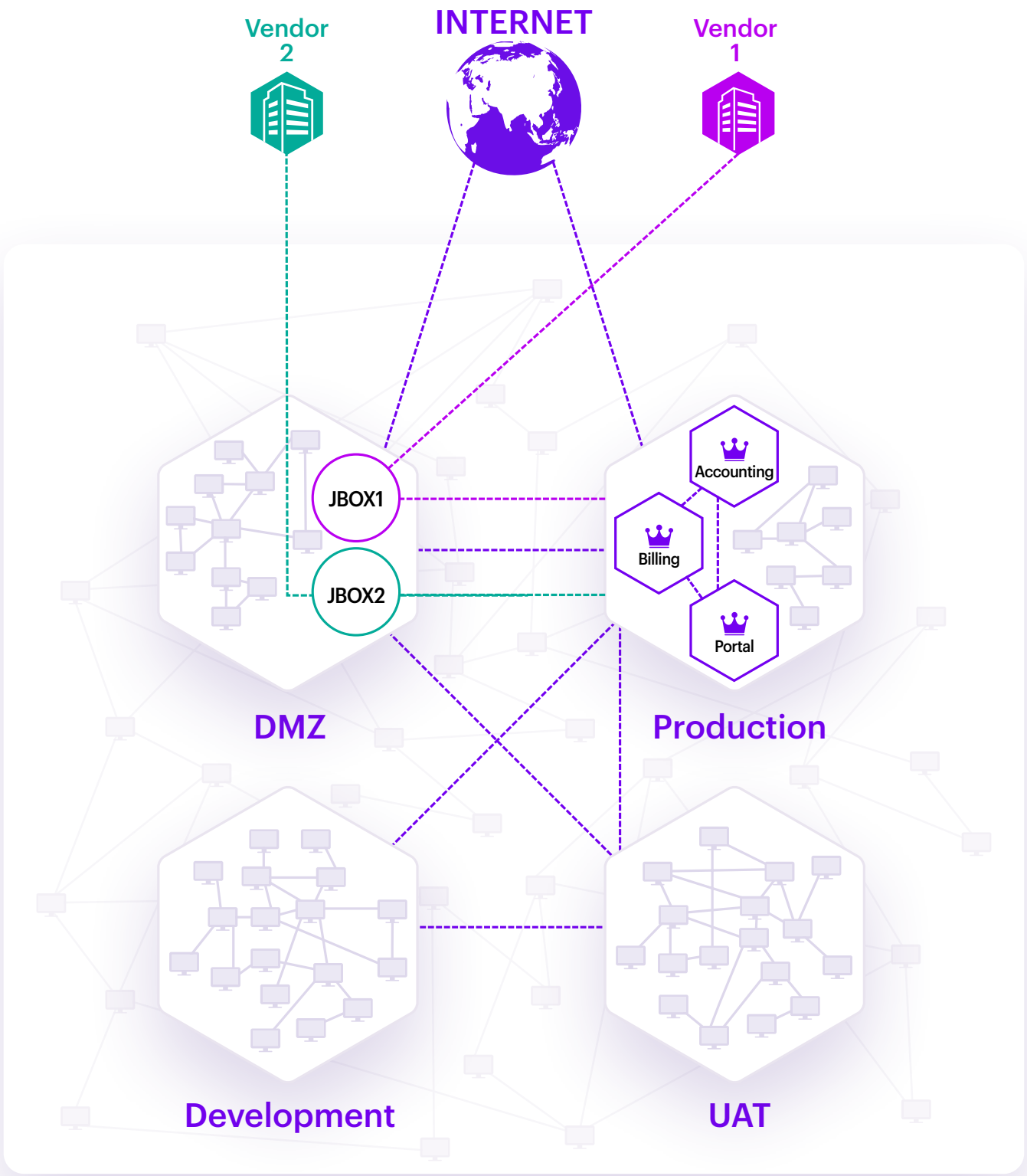
## The Guardicore Centra Security Platform
### Simplifying and Accelerating Segmentation

The bank deployed Guardicore across multiple regions and IT infrastructure types, including container technology. Because there was no need for application changes, it caused no downtime in the production environment. It also allowed the bank to quickly achieve centralized visibility into data center workloads and isolate the Production, Test and Development environments. Using Guardicore, the customer was also able to restrict access to servers from printers, other IoT devices, and unauthorized users.

In less than three months, the project was completed. It went 10x times faster than initially estimated with traditional segmentation methods. By quickly mapping out the environment and creating policies based on the collected information, the bank improved its security posture and addressed the compliance requirements for more than 10,000 non-compliant assets. The speedy deployment resulted in risk reduction, significant cost and resource savings.

Guardicore's professional services team helped the bank to completely transform their segmentation processes. Today the assets labeling and segmentation policies are fully automated, embedded in the application development and deployment processes. The labels creation, change management, security incidents and service requests are fully integrated into the ServiceNow workflows.

The customer was extremely satisfied with the results from the platform and the value it delivered along with Guardicore's partnership attitude and the vendor's skilled and dedicated technical services teams.




*Environments segmentation and third party access control with Guardicore.*

**Want to learn more about Guardicore Centra? Visit www.guardicore.com today**

## About Guardicore

Guardicore is an innovator in data center and cloud security that protects your organization's core assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security for any application, in any IT environment. www.guardicore.com

Guardicore