Akamai

WHITE PAPER

Crush Cybersecurity Roadblocks with Software-Based Segmentation

Akamai Guardicore Segmentation helps improve access security and reduce cyber risk costs in the European financial sector

Overview

The financial sector is a crucial part of the European Union's economy, and financial systems are considered critical infrastructure by some European governments and regulators. The products and services provided by financial services organizations depend heavily on highly available IT systems and in-time access to information delivered through multiple channels and parties.

However, ransomware and cryptomining attacks have shown how quickly threat actors can disable this critical infrastructure for days, or even weeks, possibly spreading to connected third parties and peers.

It's vital that European financial institutions embrace cutting-edge digital capabilities in the pursuit of competitiveness, customer acquisition, and retention. Yet the increasing regulatory requirements for security controls and reporting are significantly slowing down the rate of cloud adoption. The European Union's General Data Protection Regulation (GDPR), for example, may levy fines of up to 4% of global turnover against companies that fail to protect their customers.[1]

In addition, recent regulations such as the Society for Worldwide Interbank Financial Telecommunication Customer Security Programme (SWIFT CSP) and the European Central Bank's cyber resilience oversight expectations (ECB CROE) specifically call for more granular network segmentation.

Traditional segmentation approaches and their associated manual procedures are not a viable approach to keep up with the pace of technological innovation, increased security risks, and ever-tightening regulations.

Organizations need to not only adopt new tools but also fundamentally change their security and segmentation processes to embrace simplicity, transparency, and automation.

This paper will cover:

- The key cybersecurity challenges the European financial sector faces today
- How banks and financial institutions can address these risks with a cost-effective and straightforward approach to segmentation
- How Akamai Guardicore Segmentation's approach helps companies simplify their security processes, significantly reducing costs and accelerating compliance

Today's cybersecurity is complex and costly to navigate

Though European banks and financial institutions are committed to organizational security and protecting customers' data, navigating the path to a stronger security posture is not an easy journey in today's world of evolving risks, third-party access needs, and compliance requirements.

Increased cyber risk increases monetary losses

The risks associated with cybercrimes are particularly severe for financial institutions. The financial industry is already spending the second-most of any industry fighting off attacks, with an average cost of $5.72 million per data breach.[2]

Yet achieving a strong security posture is also expensive. Enforcing security controls to protect not only multiple platforms but also third-party access — which is critical to business service delivery — is a complex task. It comes with a significant increase in infrastructure and labor costs.

Compliance is costing more

Financial services organizations in Europe have seen a dramatic increase in the cost, time, and overall resources needed to prepare for and validate compliance. While regulations help ensure the stability of the financial sector, the continual introduction of new cybersecurity mandates is impacting profitability and growth by slowing down digital transformation and requiring substantial investments.

Increased pressure to tighten up policies started with the GDPR and was followed by the Directive on Security of Network and Information Systems (NIS), ECB CROE guidance, and, most recently, the EU Cybersecurity Act. Altogether, with the addition of vendor mandates such as SWIFT CSP, achieving compliance today means addressing a vast number of reporting and technical requirements.

Therefore, as they upgrade their technology, banks and financial institutions also need to find ways to simplify management and lower the operational costs related to cybersecurity and compliance.

Security vulnerabilities of third-party and financial market interactions

The EU's revised Payment Services Directive (PSD2), aimed at improving user convenience and transparency, amplified the risks of third-party access and personal data compromise. There is also growing pressure, from financial services peers and regulators, for efficiency and transparency regarding business and technology processes.

Additional demands from customers around security, mobility, and new services have led to an increased dependence on third-party information and communications technology infrastructures, outsourcing providers, and their supply chains.

As environments become more connected than ever, protecting all types of communications, including automated inter- and intra-banking transactions, has become resource-intensive.

Now, a single breach to one party's data center could have a domino effect, as attackers would only need to exploit a single asset to move laterally between interconnected parties, including peer financial institutions and financial markets, putting the security and business continuity of the entire European financial services ecosystem at risk.

The hybrid cloud requires a new security approach

Compliance mandates, along with the European Bank Authority[3] guidelines, are shaping cloud adoption trends in the financial sector. While cloud adoption is on the rise in Europe, regulations have increased the complexity of migrating on-premises systems to the cloud.

Because of this, European companies are more likely to keep core functions on-premises and embrace hybrid cloud environments rather than all-cloud environments. Many banks have also advanced to using several cloud service providers, resulting in a multicloud infrastructure.

However, organizations are typically seeking more than just increased security. They're also looking for cost savings and improving operational efficiency through process modification. Automation and process modernization become key to success.

Address key cybersecurity challenges with network visibility and segmentation

The theme running through these challenges is a need to securely isolate critical applications and workloads — commonly referred to as segmentation. This allows financial institutions to achieve security at scale according to business needs and demonstrate a risk-based approach that is in line with regulatory requirements.

Legacy firewalls are not the answer

There are several reasons segmentation hasn't been more widely embraced and deployed at European banks and financial institutions.

Maintenance and resource intensity: Many security and IT professionals are hesitant to pursue segmentation initiatives, citing that they take too long and tie up multiple teams and tremendous amounts of resources. This hesitancy is understandable, since traditional methods tend to be both complicated and time-consuming. For example, configuring VLANs, ACLs, and firewalls across multiple locations and environments is quite often a laborious, slow, and error-prone process. Also, traditional methods rely heavily on unreliable identity data, such as IPs, which have little meaning and can frequently change.

Lack of visibility: Organizations are further stymied by a lack of visibility into east-west traffic, making it difficult to identify intersegment dependencies and create segmentation rules that won't break critical components. Even when using traffic taps or similar technologies, the resulting view often lacks the context and the sophisticated translations needed between IPs and ports. In dynamic environments, such as platform as a service (PaaS), it's all but impossible.

Infrastructure dependence: If workloads extend into the cloud, which is increasingly common, the process becomes even more complicated. Placing a hardware firewall at every data egress point is cost-prohibitive. Further management challenges arise with the complex networking configurations. These configurations are required to meet the demands of diverse environments with virtualized or legacy assets in addition to cloud and containers.

> "In some areas, the regulatory regime has struggled to maintain pace with technological innovation, but so too have firms' risk management and control frameworks."
>
> — Financial Markets Regulatory Outlook 2023, Deloitte's EMEA Centre for Regulatory Strategy

Introduce fundamental process change

Even medium-sized financial services organizations with a few hundred servers can generate thousands of segmentation policy line items. Manually managing these is ineffective, especially in environments with automated application delivery, using tools like Jenkins and CI/CD cycles where context is critical.

That's why Akamai Guardicore Segmentation goes one step further, helping organizations shift their policy creation and update cycles from a fundamentally manual process to an automated one.

With Akamai Guardicore Segmentation, once an application's profiling is automated and all dependencies are mapped, rule creation and updates can be turned into a repeatable process where stakeholders and application owners only need to approve automatically generated policies. This almost eliminates the need for manual intervention, which can slow down projects significantly, and reduces the risk of misconfigurations and human error.

Automated rule creation maintains the structural consistency of the rules and the scalability of the policy itself, leading to more optimized firewalling.

Accelerate IT transformation to build a true Zero Trust environment

Financial institutions should not let manual processes and limited resources hold them back from achieving segmentation at scale. True Zero Trust requires not only the right technology but also modernization of security policy creation, change, and maintenance processes.

Host- or software-based firewalls have emerged as a straightforward and cost-effective approach to application-level security. This approach dramatically accelerates implementation, simplifies ongoing maintenance, and is ultimately more effective in mitigating threats. Akamai Guardicore Segmentation is built from the ground up to help make segmentation simple, cost-effective, and faster for organizations of all sizes.

It provides a visual map of all applications in the data center and their dependencies. Security operators can then create and enforce network and individual process-level security policies to isolate and segment critical applications and assets. This software-defined overlay approach is independent of the underlying infrastructure and protects workloads that span on-premises legacy systems, VMs, containers, clouds, and more. Policies can be created around individual or logically grouped applications, regardless of where they reside. These policies dictate which components can and cannot communicate with each other, creating the foundation for a Zero Trust approach to security.

Efficiently reduce cyber risks and costs

Financial institutions that use Akamai Guardicore Segmentation find that they can address some of their most pressing security concerns while reducing cost in a short period:

Reduce costs of cyber risks by enforcing network security hygiene and best practices in increasingly complex and interconnected environments.

Simplify compliance management via granular contextual visibility and segmentation policies to quickly map and isolate compliance-related assets and business-critical applications. By using a single-pane-of-glass approach, a financial institution can reasonably demonstrate it is taking measures to secure critical assets, mitigate fraud risk, and protect customer privacy.

Protect third-party access by enforcing routes for third-party traffic with identity-based segmentation, isolating and restricting users from traveling across a network. This hardens security around third-party and financial market interactions, preventing attackers from "landing and expanding" from another compromised system.

Isolate money transfer and payment systems from general IT to meet the requirements of electronic funds transfer and payment systems, notably SWIFT, for strict separation of SWIFT services from an institution's general IT environment. Granular segmentation enables banks' IT teams to set context-based (user, domain) boundaries around a service provider's "zone" to further restrict unauthorized access.

Migrate to the cloud securely and quickly by mapping workloads and taking inventory of all critical applications and their dependencies before migration. Ringfencing policies can use these maps as a foundation for consistent security that follows the workloads throughout the migration process. This approach enables faster and more secure cloud migration, keeping the same security controls in place regardless of application or infrastructure changes.

Ensure business continuity with efficient breach mitigation through granular visibility into east-west traffic and breach indicators to alert on abnormal movement to stop threat actors before they exfiltrate sensitive financial and customer data.

Reduce risk by limiting lateral movement. Today, the majority of data center traffic moves laterally between applications (east-west), rather than entering the data center from outside (north-south). Setting internal boundaries by ringfencing business-critical applications and systems effectively reduces the attack surface, protecting against the lateral spread of attacks and limiting damage in the event of a breach.

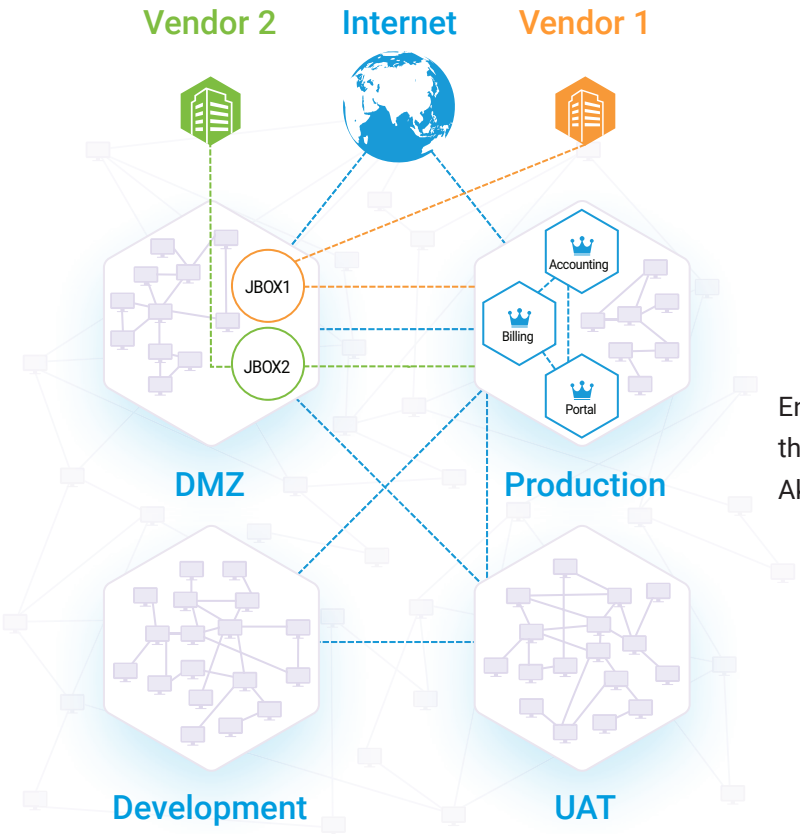
Case study: Compliance cost reduction at a large European multinational bank

A large European bank was looking for a new, efficient network segmentation approach, necessary to comply with technical requirements from multiple regulatory agencies, including the Federal Reserve Bank of NY (FRBNY), Monetary Authority of Singapore (MAS), ECB, and others.

The bank's use of traditional segmentation approaches, firewall rules, and VLANs was proving ineffective, resulting in high annual noncompliance costs. It was also impacting IT operations with significant production downtime and resources required to create and update policies.

A more cost-effective and easy-to-implement approach was needed to accomplish the bank's segmentation objectives. The key requirement for a new solution was minimal impact on the bank's infrastructure and resources, while also providing full compliance with the relevant regulations.

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: Akamai Guardicore Segmentation offered the fastest, most straightforward path to microsegmentation.



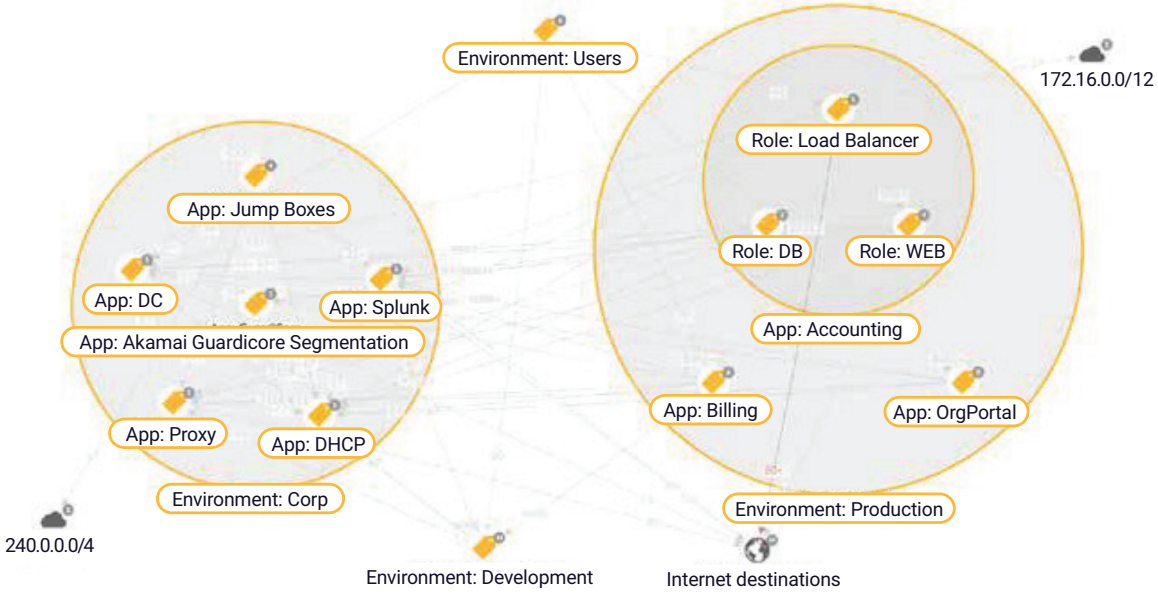
Environment segmentation and third-party access control with Akamai Guardicore Segmentation

Simplifying and accelerating segmentation

The bank deployed Akamai Guardicore Segmentation across multiple regions and IT infrastructure types, including containers. Because there was no need for application changes, it required no downtime in the production environment. It also allowed the bank to quickly achieve centralized visibility into data center workloads and to isolate the Production, Test, and Development environments. Using Akamai Guardicore Segmentation, 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 complete. It went 10 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 compliance requirements for more than 10,000 noncompliant assets. The speedy deployment resulted in risk reduction, as well as in significant cost and resource savings.

Akamai's professional services team helped the bank to completely transform segmentation processes. Today, the asset labeling and segmentation policies are fully automated, embedded in the application development and deployment processes. The label 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 Akamai's skilled and dedicated technical services teams.



Learn more about Akamai Guardicore Segmentation at akamai.com/guardicore

1 "What are the GDPR Fines?" GDPR.eu, February 13, 2019.

2 "Cost of a data breach 2022," IBM.

3 "A comprehensive guide to cloud adoption in Europe's banking sector," Techerati, October 31, 2019.