Guardicore

CRUSH CYBERSECURITY ROADBLOCKS WITH SOFTWARE-BASED SEGMENTATION

Guardicore Centra helps improve access security and reduce cyber risk costs in European Financial Sector

White Paper

OVERVIEW

"Cybersecurity is already important, and it will become even more significant for institutions and their regulators in the future. The challenge will be to balance safety with customer convenience. For full-scale providers who are trying to maintain visibility across channels, this is harder than it looks."

Financial Services Technology 2020 and Beyond, PwC, 2020

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 organisations heavily depend on highly available IT systems and in-time access to information delivered through multiple channels and parties.

However, recent ransomware and crypto-mining attacks have shown how quickly these infrastructures can be disabled by bad actors for days, or even weeks, possibly spreading to connected third parties and peers.

Research by the European Union Agency for Network and Information Security (ENISA) goes on to explain that, "such impacts will not be confined to the "virtual" world; a major attack outreach would most certainly impact the assets in safekeeping or in transit." [1]

It is also 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.

In addition, recent regulations such as SWIFT CSP and 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 technology innovation, increased security risks, and 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:

- What 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 Guardicore's approach helps companies simplify their security processes, significantly reducing costs and accelerating compliance

[1] "Network and Information Security in the Finance Sector", ENISA, January 15, 2015

TODAY'S CYBERSECURITY IS COMPLEX AND COSTLY TO NAVIGATE

Though European banks and financial institutions are committed to organisational 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 International Monetary Fund (IMF) estimated, conservatively, that the total average annual aggregate losses due to cyber risk to the industry equal approximately 9% of its net income, or USD 100 billion (The IMF suggested that potential losses of this magnitude represent a possible threat to global financial stability).[2]

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

Compliance Is Also 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 from organizations.

Increased pressure to tighten up policies started with the General Data Protection Regulation (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, in the journey towards digitisation, banks and financial institutions also need to find ways to simplify management and lower the operational costs related to cybersecurity and compliance.

[2] "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment," Antoine Bouveret, June 22, 2018, January 15, 2015

Security Vulnerabilities of Third-Party and Financial Market Interactions

The EU Directive on Payment Services (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 dependency on third-party information and communications technology (ICT) 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 centre 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 (EBA)[3] guidelines are shaping cloud adoption trends in the financial sector.

"Numbers show a slow rise in cloud adoption among European enterprises, including in financial services. According to Eurostat, 26 percent of enterprises were using cloud computing in December 2018. Despite a sizable increase compared to 2014 (19 percent), the numbers do not mirror the rise in sophistication of cloud itself over the same period. In part, this difference is linked to the complexity of cloud migration under existing regulation, especially in the financial sector."[4]

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 multi-cloud infrastructure.

However organizations need more than just a solution that can increase security. There is also a substantial requirement for cost-savings and improving operational efficiency through process modification. Here automation and processes modernization is a key to success.

[3] EBA Guidelines on Outsourcing Arrangements, EBA, 25 February 2019

[4] A comprehensive Guide to Cloud Adoption in Europe's Banking Sector", Techerati, October 31, 2019

ADDRESS KEY CYBERSECURITY CHALLENGES WITH NETWORK VISIBILITY AND SEGMENTATION

"Firms will need to demonstrate they have considered, and can manage, the full range of technology and resilience risks they face, especially as they upgrade their core systems to be able to innovate."

Financial Markets Regulatory Outlook 2020, Deloitte's EMEA Centre for Regulatory Strategy, 2020

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 Intensive: Many security and IT professionals are hesitant to pursue segmentation initiatives, citing that they take too long and tie up multiple teams and resources. This hesitancy is understandable since traditional methods are both complicated and time-consuming. For example, configuring VLANs, ACLs, and firewalls across multiple locations and environments is 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: Organisations are further stymied by a lack of visibility into East-West traffic, making it difficult to identify inter-segment dependencies and create segmentation rules. Even 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 Dependent: 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.

Introduce Fundamental Process Change

"Automation is seeing significant and growing usage, with nearly two thirds of companies using it now for some cybersecurity activities, and many considering extensive use soon."

IIF/McKinsey Cyber Resilience Survey, Mckinsey & Company, March 2020

Even medium-sized financial services organisations 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 Guardicore goes one step further, helping organizations shift their policy creation and update cycles from a fundamentally manual process to an automated one.

With Guardicore, once an applications' 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 into True Zero Trust Environment

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

In recent years, 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. A leading example of this is the Guardicore Centra® Security Platform, built from the ground up to help make segmentation simple, cost-effective, and faster for organisations of all sizes.

Guardicore provides a visual map of all applications in the data centre 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 across on-premise legacy systems, VMs, containers, and clouds.

Policies can be created around individual or logically grouped applications, regardless of where they reside in the data centre. These policies dictate which can and cannot communicate with each other, creating the foundation for a Zero Trust framework.

Efficiently Reduce Cyber Risks and Costs

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

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 bank IT teams to set context-based (user, domain) boundaries around a service provider's "zone" to further restrict unauthorized access.

Adopt the cloud securely and quickly: by mapping workloads and taking inventory of all critical applications and their dependencies before migration. Ring-fencing 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 bad actors before they exfiltrate sensitive financial and customer data.

Reduce risk by limiting lateral movement: Today, the majority of data centre traffic moves laterally between applications (East-West), rather than entering the data centre from outside (North-South). Setting internal boundaries by ring-fencing business-critical applications and systems reduces attack surface effectively, protecting against the lateral spread of attacks and limiting damage in the event of a breach.

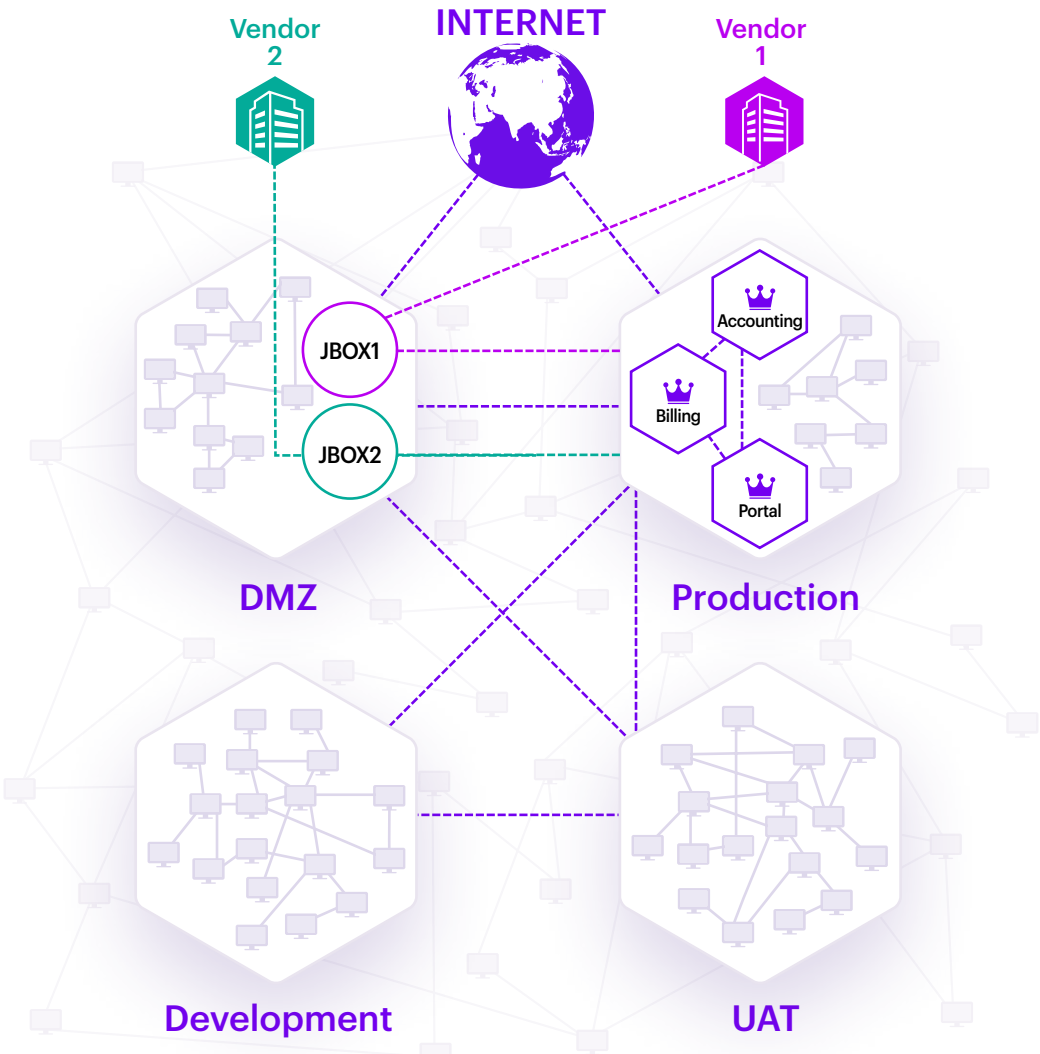
CASE STUDY: COMPLIANCE COST REDUCTION AT LARGE EUROPEAN MULTINATIONAL BANK

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), European Central Bank (ECB), and others.

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

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: Guardicore's technology offered the fastest, most straightforward path to micro-segmentation.



Environments segmentation and third party access control with Guardicore.

SIMPLIFYING AND ACCELERATING SEGMENTATION WITH THE GUARDICORE CENTRA SECURITY PLATFORM

The bank deployed Guardicore across multiple regions and IT infrastructure types, including containers. 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 centre 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 skilled and dedicated technical services teams.