Guardicore

CYBERSECURITY FOR COMMUNITY BANKS AND CREDIT UNIONS

SIMPLIFYING AND ACCELERATING SEGMENTATION FOR CRITICAL ASSETS & APPLICATIONS

White Paper

“Customers are becoming increasingly aware of cybersecurity threats and they expect their banks and credit unions to secure and protect their private financial information.”

Community banks and credit unions play a vital role in the country’s financial system. In the face of strong competition from larger banks, they seek to differentiate themselves by delivering a more personalized banking experience. At the same time, they face unique technology and information security challenges that affect their ability to compete and grow. Working with limited resources compared to their larger competitors, they must find simple and creative solutions to reduce risks, meet compliance requirements and safely embrace new technologies.

These days, customers expect their local banks to deliver their services above and beyond any large national brand bank – with a more personalized experience while also with the expectation that their personal data is secured and protected. As stated in a report from the Financial Services Information Sharing and Analysis Center’s Credit Union Council, “Customers are becoming increasingly aware of cybersecurity threats and they expect their banks and credit unions to secure and protect their private financial information.”[1] Also, banks have validated this trend by reporting that losses due to operational disruption and losses in customer trust are more financially damaging than losses due to regulatory fines.[2]

Community banks strive for security controls that measure up to those of their major competition, yet they face obvious resource constraints. As a recent Security Magazine report put it, “Although threats and risks are equal and agnostic, size does matter when it comes to resources financial organizations use to prepare for, and respond to, cybersecurity issues.[3]

> *“89 percent of banks rank enhancing cyber and data security as a top priority for the current year.”*
>
> “Global Banking Outlook 2018,” EY, 2018

UNIQUE SECURITY CHALLENGES

As they seek to achieve security at scale, community banks face challenges in five key areas:

Attackers frequently exploit weak third-party connections to gain access to a bank’s network

Third-party access: Smaller banks are often reliant on a network of partners, service and data providers. They need the means to isolate, protect and enforce third-party access routes, while limiting access only to approved applications, systems and environments – all without sacrificing flexibility. Attackers frequently exploit weak third-party connections, including access through IoT devices, to gain access to a bank’s network and start moving laterally.

[1] “Credit Union Council (CUC),” FS-ISAC, 2019

[2] Deloitte & FS ISAC Cybersecurity Benchmarking Analysis, 2019

[3] “How Risk-Based Cybersecurity Programs Differ Between Community & Global Banks,” Security Magazine, May 3, 2018

Cost reduction: Finding business practices and technologies that enable cost savings is paramount to community banks. A juxtaposition to innovation, community banks always weigh cost savings as a factor in their IT and business initiatives.

ABOUT 15 DIFFERENT AGENCIES
impose cybersecurity requirements on banks

Cybersecurity compliance: While community banks generally look to the FDIC for cybersecurity guidance, there are about 15 agencies on federal, state and local levels that impose additional cybersecurity requirements. Recent years have seen a number of high-profile cases in which criminals have compromised electronic funds transfer and payment systems, not by penetrating those systems themselves, but by gaining access through the client bank's network. Therefore, third-party core banking service providers often include specific cybersecurity requirements in their contracts. Banks must figure out how to efficiently address these requirements and regulations.

Reduce IT footprint by moving operational workloads to the cloud and adopting cutting edge technologies

Cloud migration and new technologies: Community banks and credit unions are looking to reduce their IT footprint and gain operational efficiency by moving their operational workloads to the cloud, often combining on-premise data centers with private or public clouds. They are further looking to create a differentiated digital customer experience with cutting edge technologies. In fact, cloud adoption has been the top ranked emerging technology, irrespective of organizational size, cybersecurity maturity or cybersecurity budget.[4] Banks must be aware of and take measures to mitigate the security risks that accompany new technology adoption.

43%
of breaches in 2019 targeted smaller organizations

Breach mitigation: It's no surprise that financial institutions are prime targets for cyber criminals, who are looking not only for easy money but also for the wealth of private information that customers entrust to their banks. Perimeter defenses are essential, but unfortunately, breaches have become business as usual. While a larger organization might be able to weather the storm after a breach, the fallout and reputational damage can be devastating to a community bank. In fact, an estimated 43% of breaches in 2019 targeted smaller organizations.[5] Furthermore, 9 out of 10 organizations experienced sensitive business production data disclosures. Top threats indicate the need to protect data and applications, including in the expanded enterprise.[6] As the modern perimeter becomes harder to define and defend in a hybrid infrastructure, community financial organizations need to take measures to mitigate the impact of breaches by preventing intruders' lateral movement and ring-fencing their critical assets.

> *"Each global financial institution, community-focused bank and credit union is a high-value target for potential cyber events. However, for smaller organizations, regulatory pressures, staffing needs and budget realities make staying safe and compliant particularly challenging."*
>
> "How Risk-Based Cybersecurity Programs Differ Between Community &amp; Global Banks," Security Magazine, May 3, 2018

[4] Deloitte & FSI ISAC Cybersecurity Benchmarking Analysis, 2019

[5] "2019 Data Breach Investigations Report," Verizon, 2019

[6] Deloitte & FSI ISAC Cybersecurity Benchmarking Analysis, 2019

VISIBILITY AND SEGMENTATION ADDRESS KEY CHALLENGES IN COMMUNITY FINANCIAL INSTITUTIONS

The common theme running through these challenges is the need to separately secure critical application workloads and many of their third party provided applications and infrastructure – commonly referred to as segmentation. It allows community financial institutions to achieve security at scale by addressing several key requirements, while still moving at the speed with their business demands.

Secure cloud adoption: Lack of visibility into network traffic and digital assets can make the move to the cloud virtually impossible. As a starting point in the digital transformation journey, community banks need to have an accurate inventory and map of all their core and critical applications, their dependencies and the network traffic they generate. This visibility will provide a foundation for the ring-fencing controls to allow seamless migration of the applications into the cloud, along with their security policies.

Protecting third-party access: Third-party outsourcing or software provider traffic needs to be properly routed, usually through a "jump-box" in the DMZ to a single termination point within the data center and be restricted from traveling across the bank's network. This is essential to prevent attackers from "landing and expanding" through a third party's compromised system.

Isolating money transfer and payments systems from general IT: Providers of electronic funds transfer and payment systems, notably the Federal Reserve's FedLine service, typically demand strict separation of their services from the institution's general IT environment. Segmentation enables bank IT teams to set boundaries around the service provider's "zone" and prevent unauthorized access.

Reducing risk by limiting lateral movement: Today, the majority of data center traffic is lateral between applications (east-west) rather than entering the data center from outside (north-south). With flat networks, the reality at many organizations, it only takes a breach of a single machine to give bad actors a foothold from which to access sensitive applications and data. Segmentation can effectively protect against lateral movement and reduce risk by ring-fencing business-critical applications and systems.

Addressing compliance and cyber regulation: Segmentation gives banks an efficient way to comply with both the vendor requirements and cybersecurity regulations from multiple agencies. Accompanied by deeper visibility with a single pane of glass, it allows them to demonstrate that they are taking effective measures to secure critical assets, mitigate fraud risk and protect customer privacy.

Cost Reduction: When done correctly, segmentation can actually reduce costs community banks face. The key word is correctly. To understand what it is to do segmentation correctly, one must first look in the next section how it should and should not be done.

WHERE CONVENTIONAL SEGMENTATION APPROACHES FALL SHORT & WHERE SOFTWARE DEFINED SEGMENTATION SUCCEEDS

If segmentation answers many of the challenges facing community banks and credit unions, why hasn't it been more widely embraced and deployed? Many CISOs at smaller institutions are hesitant to pursue segmentation initiatives, citing that they take too long and require multiple teams and resources. This hesitancy is understandable. Traditional methods of achieving segmentation 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. If workloads extend into the cloud, the process is complicated significantly. Placing a firewall at every data egress point is cost-prohibitive, and further management challenges arise with the complex networking configurations required to route traffic and place firewalls in virtual environments.

Traditional methods of achieving segmentation are both complicated and time-consuming

Organizations are further stymied by a lack of visibility into east-west traffic, making it difficult to identify inter-segment dependencies and create segmentation policies. Even using traffic taps or similar technologies, the resulting view likely lacks the context and sophisticated translations between IPs and ports required for effective segmentation. In dynamic environments, such as platform-as-a-service (PaaS), it's all but impossible.

A Different Approach

In recent years, software-defined segmentation has emerged as a more flexible, streamlined and cost-effective approach to application-level security, one that dramatically accelerates implementation, simplifies ongoing maintenance, and is ultimately more effective in mitigating threats. A leading example of this methodology is the Guardicore Centra® security platform. Guardicore takes the concept of segmentation to a very granular level, enabling the creation of security policies around individual or logically grouped applications, regardless of where they reside in the hybrid data center. These policies dictate which applications can and cannot communicate with each other – true zero trust at the application level.

Segmentation with Guardicore allows for protection of applications, threat detection and prevention of lateral spread of attacks

Besides protecting applications from malicious access, software-defined segmentation with Guardicore has the additional benefit of threat detection and preventing the lateral spread of attacks. Any attempt at unauthorized communication is an instant indicator of the likely presence of a threat.
To affect this level of segmentation, Guardicore provides a visual map of all applications running in the data center and the dependencies among them. Operators can then create and enforce network and individual process-level security policies to isolate and segment critical applications and assets. With a software-defined overlay approach, it is independent of the underlying infrastructure and protects workloads that span on-premise facilities, legacy systems, VMs, containers and clouds.

This simplifies and accelerates segmentation efforts by:

- Detecting and interpreting workload dependencies automatically at the process level, with additional identity and domain name granularity
- Enforcing one consistent policy expression as applications migrate across heterogeneous environments with zero changes to infrastructure
- Avoiding application modifications and production downtime through a software-defined overlay approach
- Future-proofing policies with platform-independent contextual traffic visibility and segmentation
- Ensuring and continuously validating compliance with real-time and historical traffic visibility

With Guardicore, community banks can address the most pressing security concerns simply, efficiently and in a short period of time

Community banks and credit unions that use Guardicore to segment their environment find that they can address some of their most pressing security concerns simply, efficiently and in a short period of time. Guardicore enables these institutions to:

- **Apply IoT and third-party access controls** that isolate access routes and reduce the exposed attack surface
- **Meet compliance mandates** by quickly mapping and separating compliance-related systems and assets and ring-fencing business-critical applications
- **Securely adopt the cloud and new technologies** with consistent security policies that support all existing and evolving infrastructures
- **Mitigate the impact of breaches** through granular visibility into east-west traffic and stopping the lateral movement of bad actors before they exfiltrate financial data

Secure the Benefits of Digital Transformation

Community financial services organizations should not let limited resources hold them back from achieving security at scale. Guardicore was built from the ground up to help make segmentation simple, cost-effective and faster for organizations of all sizes. Segmentation with Guardicore enables community banks and credit unions to accelerate their digital transformation and compete more effectively.

> *"Minimizing overall cyber risk to the financial sector depends upon the protection and participation of smaller organizations such as credit unions, savings banks, building societies, trust companies, account servicers, and even end customers. A system's cybersecurity is only as strong as its weakest links."*
>
> "Capacity-Building Tool Box for Cybersecurity and Financial Organizations," The Carnegie Endowment for International Peace, July 2019"

CASE STUDY:
SPEEDING THE TRANSITION TO HYBRID-CLOUD

A community bank located in the midwestern US was looking to securely adopt hybrid cloud while strengthening controls over third-party access and ring-fencing critical applications and systems. With limited IT resources, they were looking for a solution that would allow them to accomplish these objectives with minimal impact on their infrastructure and resources while providing maximum cyber-risk reduction.

The project specifically targeted the bank's digital "crown jewels": Ten critical applications requiring ring-fencing and preparation for migration. In addition, they needed to completely isolate the FedLine environment from the general IT infrastructure, in line with the requirements of the Federal Reserve Bank, the provider of the FedLine Services.

With Guardicore, the team was able to:

- Gain granular visibility into east-west traffic, with a "single pane of glass" view of all applications and assets regardless of their location and environment
- Inventory all applications and their dependencies quickly and accurately
- Migrate applications between environments without creating service disruptions
- Implement a unified security standard across the hybrid infrastructure

Guardicore helped this mid-size financial institution become cloud-ready without putting extra stress on their limited IT resources and without any impact on the underlying infrastructure.

Had the IT and security teams chosen to go the VLAN or firewalling route, they estimated the project would have taken a full team 18 months, without any gain in visibility or third-party access restrictions. With Guardicore, they completed all the project's objectives in two months with only one information architect. More importantly, the bank was able to start reaping the benefits of the cloud and operational cost savings more quickly.

> *"Guardicore has provided us with the fastest and most elegant path to application segmentation while delivering the added benefit of breach detection for lateral traffic."*
>
> - Chief Information Technology Officer, Mid-size Regional U.S. Bank

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 presistent and consistent security for any application, in any IT enviornment. www.guardicore.com

v.2.0

Guardicore