AKAMAI SOLUTION BRIEF

Segmentation Designed for Credit Unions

Credit unions face a relentless wave of cyberthreats, from ransomware to phishing, that jeopardize member data and operational stability. As resource-constrained organizations, credit unions must carefully choose security capabilities that provide maximum return on risk reduction and balance robust security with regulatory compliance and innovation.

Software-defined segmentation, exemplified by tools like Akamai Guardicore Segmentation, offers a modern approach to protect critical systems, isolate high-value assets, and meet compliance requirements. By limiting lateral movement and enhancing visibility, credit unions can reduce risk of major impact to operations without hindering the growth of the business.

Akamai Guardicore Segmentation highlights

- Reduce lateral movement in record time
- Meet NCUA/FFIEC compliance needs
- Visualize east-west traffic
- Control third-party access
- Support hybrid cloud adoption
- Protect member-facing services

What is software-defined segmentation?

Software-defined segmentation is a dynamic cybersecurity strategy rooted in Zero Trust principles outlined in NIST Special Publication 800-207. Traditional perimeter-based strategies, like static firewalls and VPNs, often fail to limit lateral movement once an attacker gains access to a network. Software-defined segmentation, on the other hand, deploys lightweight software agents to create policies that follow workloads across on-premises, cloud, containerized, and legacy environments. These policies define which applications, services, or processes can communicate, aligning with the Zero Trust principle of least-privilege access.

For credit unions looking to strengthen security without disrupting operations, software-defined segmentation is an impactful, practical solution. This approach:

- Isolates member services to safeguard sensitive data
- Secures payment systems
- Restricts third-party vendor access to authorized resources
- Delivers cost-effective security
- Provides real-time visibility into network traffic
- Simplifies compliance efforts
- Rapidly mitigates and contains threats

Tools like Akamai Guardicore Segmentation enhance these benefits by automating policy enforcement and providing visual traffic maps, enabling rapid threat detection and response.

When should credit unions use segmentation?

Segmentation is essential for credit unions when protecting sensitive member data, ringfencing critical services like payments and core banking, and minimizing risk from third-party vendors. It also supports Zero Trust security initiatives and helps institutions meet guidance from NCUA and FFIEC. With software-defined segmentation, credit unions can move quickly — no matter how complex or hybrid their IT environment.

Why segmentation is a good strategy

Credit unions are no strangers to cybersecurity challenges. But with limited budgets and lean teams, they have to be strategic. That's why many are turning to high-impact solutions like software-defined segmentation. Akamai customers point to its ability to boost visibility, ease compliance, and contain threats without stretching resources thin. Here's how segmentation helps tackle today's top risks:

- **Limit vendor risks:** Segmentation isolates third-party access routes, reducing exposure from vendor-related incidents.
- **Reduce staffing needs:** Automated policy enforcement minimizes reliance on dedicated cybersecurity staff.
- **Ensure compliance:** Granular policies and audit reports meet NCUA's Part 748 and FFIEC's 2021 guidance with minimal effort.
- **Secure cloud transitions:** Traffic mapping enables safe hybrid cloud adoption by identifying and protecting workloads.
- **Contain breaches:** Ringfencing critical assets stops lateral movement, mitigating ransomware and data breaches.

> "[Akamai] has provided us with the fastest and most elegant path to application segmentation, while delivering the added benefit of breach detection for lateral traffic."
>
> **— IT Security Leader at Regional Financial Institution**

Software-defined segmentation in action

Credit unions manage complex environments with limited resources, making it essential to prioritize security strategies that deliver maximum impact with minimal disruption. Now let's take a closer look at how Akamai Guardicore Segmentation addresses those challenges in real-world credit union environments — securing critical systems, simplifying compliance, and strengthening resilience against evolving threats.

- **Mitigating ransomware spread:** By limiting east-west movement, Guardicore helps credit unions stop ransomware before it reaches core systems. If an endpoint is compromised, segmentation can quarantine affected services instantly.
- **Protecting critical systems:** Whether it's FedLine, loan processing, or member-facing apps, segmenting these assets helps prevent unauthorized access and contains potential breaches before they impact operations or data.
- **Compliance and audit prep:** Segmenting networks and systems supports regulatory requirements around data privacy and access control. With real-time maps and historical traffic records, IT teams can demonstrate compliance and streamline audits.
- **Hybrid cloud enablement:** As credit unions migrate workloads to the cloud, Akamai Guardicore Segmentation provides visibility into dependencies and traffic patterns, allowing for secure, seamless transitions while maintaining consistent policies.
- **Third-party access control:** Credit unions often rely on multiple vendors, service providers, and data aggregators. Segmentation ensures that these partners can only access specific applications or systems through designated, monitored channels — reducing risk without impacting service.

Smarter segmentation, stronger outcomes

If segmentation answers so many challenges, why haven't more credit unions adopted it?

The answer often comes down to complexity and resources. Traditional segmentation — via VLANs, ACLs, and firewalls — is time-consuming to deploy and prone to causing operational impacts. It also fails to provide sufficient visibility into east-west traffic and many times is limited in the ways it can interact with different environments.

Software-defined segmentation with Akamai offers a different approach. It protects member data and critical systems while providing:

- Rapid deployment without infrastructure changes
- Granular visibility into lateral traffic and dependencies
- Centralized policy control across all environments
- Flexibility to support legacy, modern, and hybrid systems
- Faster audit readiness with automated reporting

Beyond protection, Akamai Guardicore Segmentation gives credit unions peace of mind. By detecting unauthorized communication and isolating threats instantly, it helps stop breaches before damage is done — without slowing down the business.

Deployment example

A large midwestern regional financial institution, tasked with protecting assets across more than 30 locations, aimed to secure 10 critical applications by reducing the attack surface, preventing lateral movement, and limiting third-party access. At the same time, they wanted to ensure cloud-readiness for Microsoft Azure migration with a robust, scalable solution.

Using software-defined segmentation, they:

- Gained visibility into east-west traffic with real-time application dependency maps
- Created granular policies to isolate and restrict vendor access to specific APIs in days
- Enforced consistent security during cloud migration, ensuring no service disruptions
- Generated audit reports to demonstrate compliance, reducing preparation time significantly

What would have taken months with traditional methods was completed efficiently, with minimal staff effort and zero operational impact.

Akamai Guardicore Segmentation supports industry best practices such as segmentation and least-privilege access, which are reinforced by long-standing guidance from NCUA and FFIEC. While Akamai Guardicore Segmentation simplifies implementation, institutions are ultimately responsible for ensuring compliance with applicable regulations.

Secure member data and reduce breach risk with Akamai Guardicore Segmentation.

© 2025 Akamai Technologies | Support | | Published 08/25