WHITE PAPER

Cybersecurity Designed for Credit Unions

Microsegmentation delivers solid ROI for lean cyber teams

Executive summary

Credit unions face growing cybersecurity challenges as known threats like ransomware and application programming interface (API)-based breaches intensify. Akamai's 2024 Year in Review revealed that 108 billion API attacks occurred over 18 months, with financial services being a prime target. Attackers exploit business logic flaws to bypass defenses, which has resulted in a need for robust, proactive strategies to protect member data and ensure resilience. Network segmentation and least-privilege access, key practices per Federal Financial Institutions Examination Council (FFIEC) guidance, enable visibility and rapid risk mitigation. Adopting streamlined segmentation enhances security, reduces compliance burdens, and mitigates breaches early without extensive resources or downtime.

Competing with big banks is no small task. While banks can leverage vast amounts of resources for cybersecurity, credit unions with limited budgets must deploy high–return on investment (ROI) controls like microsegmentation to provide equal protection and mitigation levels.

This is because customers expect their local credit unions to deliver services equal to and above those of any large national brand bank — they demand not only the assurance that their personal data is secured and protected but also a more personalized experience.

In 2024, National Credit Union Administration (NCUA) Board Member Tanya F. Otsuka highlighted the impact of cyberattacks on credit union members: "A credit union having to pay millions to a hacker to retrieve its own customers' data hurts credit union members, reduces trust in the greater system, and potentially negatively impacts the share insurance fund." Financial institutions confirm that operational disruptions and loss of customer trust cause greater financial damage than regulatory fines.

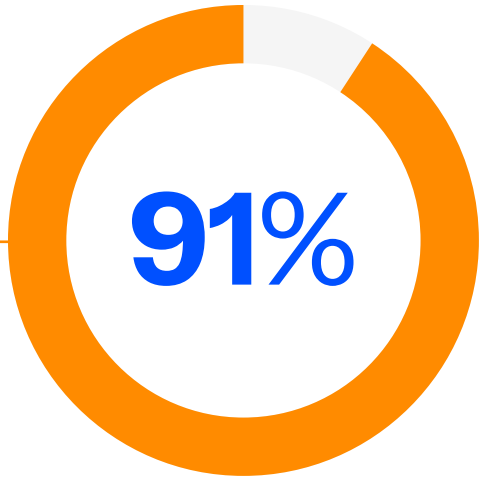
In addition to the pressure to compete while maintaining security, credit unions, along with community banks and other small organizations, face substantial resource constraints and a relentless threat landscape. “Financial institutions big and small are targeted,” said Michelle Zhang, Senior Cybersecurity Supervision Specialist for the Federal Reserve Bank of Chicago. “Threat actors may target community banks based on the belief that their cybersecurity resources and skill sets may be limited,” she added.

The threat landscape facing credit unions is growing rapidly, with ransomware, malware, phishing, distributed denial-of-service attacks, malvertising, and browser vulnerabilities being employed to disrupt operations and steal sensitive data. Emerging threats include AI-enhanced malware and sophisticated deepfake or social engineering attacks, as well as threats from supply chain and vendor software components, which can introduce vulnerabilities before deployment. Crucially, over 73% of cyber incidents involve third-party service providers and credit union service organizations that have access to a credit union’s internal network or member data.

To adapt to this rapidly evolving landscape, credit unions must adopt smarter, scalable protection.

Ransomware attacks on financial institutions have skyrocketed by **91%** since 2021, almost doubling in frequency within a few years.

Following the Money: Banking and Cybercrime in 2025



Unique security challenges

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

Ransomware
These attacks exploit data to encrypt systems and demand payment, and their number is on the rise. Microsegmentation limits lateral movement, safeguarding trust and operations.

Breach mitigation
Cybercriminals target customer data. Hybrid infrastructures blur perimeters, requiring segmentation to ringfence assets and curb breaches.

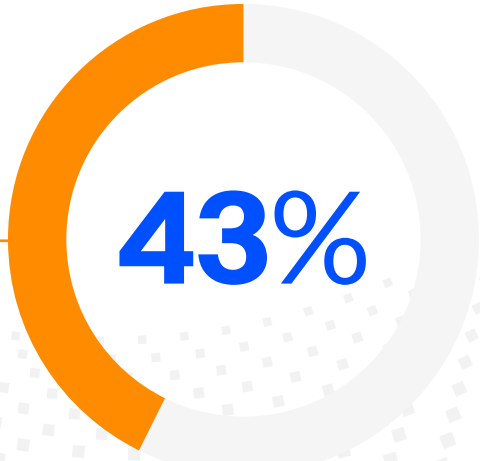
Cybersecurity compliance
NCUA's Part 748 and FFIEC's 2021 guidance mandate security programs and access controls. Credit unions must comply efficiently amid vendor demands.

Third-party access
Reliance on partners increases risk. Segmentation isolates access, limiting lateral movement via weak connections.

Cost and resource constraints
Lean budgets restrict investment. High-ROI technologies like microsegmentation enable cost-effective security.

In 2023, **43%** of cyberattacks targeted small businesses, underscoring the vulnerability of organizations with limited resources.

Must-Know Small Business Cybersecurity Statistics for 2025, BD Emerson



Cloud migration and new technologies

Credit unions adopt cloud migration, APIs, and large language models (LLMs) to boost efficiency and member services, but each introduces significant security risks. For example, financial services APIs faced 108 billion attacks in 18 months, and LLMs are vulnerable to data leakage. Microsegmentation safeguards these technologies without stifling innovation.

API protections

APIs enable seamless data exchange for member-facing apps, payments, and third-party integrations but are targeted via business logic flaws and misconfigurations. Credit unions must use API discovery to identify all APIs, enforce granular access controls, and leverage software-defined segmentation, like Akamai Guardicore Segmentation, to isolate traffic, monitor anomalies, and align with regulations.

LLM protections

LLMs drive AI-powered member services like chatbots and fraud detection but risk data leakage and manipulation. Attackers target LLMs to extract data or inject malicious prompts, threatening privacy. To ensure compliance and positive member experiences, credit unions must use strict access controls, input validation, and software-defined segmentation to isolate LLM workloads, with encryption safeguarding data.

> "Credit unions are no more immune to crime than the big banks — and with a smaller IT bench, they may present a tastier target."
>
> **Top 10 Challenges Facing Credit Unions, Engageware**

Visibility and segmentation resolve key challenges for credit unions

The common thread running through these challenges is the need to separately secure critical application workloads and the third-party applications and infrastructure they rely on — commonly referred to as "segmentation." Segmentation allows credit unions to achieve security at scale and keep pace with business demands by addressing several key requirements.

Reducing risk by limiting lateral movement: Today, the majority of data center traffic moves laterally between applications (east-west), rather than entering data centers from outside (north-south). With flat networks, the breach of a single machine is enough to give threat actors access to sensitive systems. Segmentation helps reduce this risk by ringfencing business-critical assets.

Addressing compliance and regulation: Visibility and segmentation are critical components of compliance. By mapping the environment and enforcing granular policies, credit unions can demonstrate to auditors that they've taken steps to secure member data and other sensitive information. These efforts also help credit unions avoid costly fines and build member trust by showing their commitment to security. In addition, modern segmentation tools provide reporting capabilities that streamline audit preparation, saving credit unions time and resources.

Cost reduction: Segmentation can reduce security costs and resource demands. See the next section to learn how to derive these benefits from segmentation.

Secure multicloud adoption: Lack of visibility into network traffic and digital assets can make the move to the cloud almost impossible. To begin their digital transformation, credit unions must 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 ringfencing controls, allowing applications and their security policies to be seamlessly migrated into the cloud.

Isolating payment systems from general IT: Providers of electronic funds transfer and payment systems such as the Federal Reserve's FedLine service typically demand strict separation of their services from the institution's general IT environment. Segmentation allows credit unions to establish secure zones around these systems and prevent unauthorized access from elsewhere in the network.

Protecting third-party access: Third-party software provider traffic should be routed through controlled access points — often a jump box in a demilitarized zone — to a single termination point within the data center. This routing must prevent the traffic from traversing the broader network, reducing the risk of attackers landing and expanding through compromised third-party systems.

Why conventional firewall-based segmentation approaches fall short and software-defined segmentation succeeds

If segmentation resolves many of the challenges credit unions face, why hasn't it been more widely embraced and deployed? Many CISOs at smaller institutions are hesitant to pursue segmentation initiatives, believing they require too much time and too many teams and resources.

Traditional methods of achieving segmentation, such as configuring virtual local area networks, access control lists, and firewalls across multiple locations and environments, are complicated, error prone, and time-consuming. Extending this workload to the cloud further complicates this process. Placing a firewall at every data egress point is costly, and the management challenges of routing traffic in virtual environments add complexity.

Organizations are further stymied by a lack of visibility into east-west traffic, making it difficult to identify intersegment dependencies and create segmentation policies without breaking anything. Even when traffic taps or similar technologies are used, the resulting view often lacks the context and sophisticated translations between IPs and ports required for effective segmentation. In dynamic environments, such as platform as a service, segmentation is nearly impossible.

"In the event that some other part of our cyber defense model fails, then [Akamai Guardicore Segmentation] will be the thing that saves us. Breaches happen to all businesses, and they may happen to us again. When it does, the blast zone will be far smaller, and it'll be because of Guardicore."

– Head of Infrastructure, Enabling Software

A different approach

In recent years, software-defined segmentation has emerged as a more flexible, streamlined, and cost-effective approach to securing critical assets, aligning with NCUA's Part 748 and the long-standing FFIEC guidance for segmentation and least privilege.

Akamai Guardicore Segmentation takes software-defined segmentation to a highly granular level — enabling the creation of security policies around individual or logically grouped applications and their components, regardless of where they reside in the hybrid data center. These policies dictate which components, down to individual processes, can communicate with each other — true Zero Trust at the application level.

"Is Guardicore Segmentation worth it? It's all about compartmentalizing and segmentation, which is key for any network. **The benefits of automated discovery and visualization are paramount.** When you talk about consistent deployment and less errors in deployment policies around the globe, [it's] absolutely [worth it]."

– Infosec director at a financial services organization

Besides blocking malicious access, Akamai's software-defined segmentation detects threats and helps prevent lateral attacks. Unauthorized communication triggers immediate alerts, with a visual map showing all applications and their dependencies. Operators can then enforce security policies at the network and process levels to isolate critical assets.

Because it uses a software-defined overlay approach, Akamai Guardicore Segmentation is independent of the underlying infrastructure and can protect workloads across on-premises environments, legacy systems, virtual machines, containers, and clouds. This simplifies and accelerates segmentation efforts by:

- Detecting and interpreting workload dependencies automatically at the process level, with added identity and domain name granularity
- Enforcing a consistent policy expression as applications move across heterogeneous environments — with no changes to infrastructure
- Avoiding application modifications and production downtime through a software-defined overlay
- Future-proofing policies with platform-independent contextual traffic visibility and segmentation
- Ensuring and continuously validating compliance through real-time and historical traffic visibility
- Simplifying deployment for IT staff in smaller credit unions, enabling rapid policy creation with minimal resources
- Supporting AI-driven natural language queries to streamline policy management and threat analysis for lean teams

Credit unions using software-defined segmentation find they can address their most pressing security concerns quickly, efficiently, and with minimal disruption. Akamai Guardicore Segmentation enables these institutions to:

- Apply Internet of Things and third-party access controls that isolate access routes and reduce the exposed attack surface
- Meet compliance mandates by mapping and separating regulated systems and assets and ringfencing business-critical applications
- Securely adopt cloud and emerging technologies with consistent security policies that support both legacy and modern infrastructures
- Mitigate the impact of breaches through granular visibility into east-west traffic and by stopping the lateral movement of threats like ransomware before data can be exfiltrated
- Enhance monitoring with automated threat detection, reducing the burden on IT staff in smaller credit unions
- Support lean credit union teams with intuitive tools that simplify security management and compliance reporting

Secure the benefits of digital transformation

Credit unions should not let resource limitations prevent them from achieving the same security benefits as their counterparts with scale. Akamai Guardicore Segmentation was built from the ground up to make segmentation simple, cost-effective, and faster for organizations of all sizes. Akamai Guardicore Segmentation helps credit unions and community banks accelerate their digital transformation and compete more effectively in the ever-changing threat landscape.

Learn more about our solutions for financial services.

"Smaller banks and credit unions that may lack the resources for a fully in-house security team … will need to prioritize cloud security by using encryption, implementing strict access controls, and regularly auditing their cloud environments … By 2025, third-party data breaches will continue to pose major threats to the financial sector."

Cybersecurity in 2025: What Financial Institutions Need to Know,
First Bank & Trust Company

Akamai

Akamai Security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale of our global platform and its visibility to threats, we partner with you to prevent, detect, and mitigate threats, so you can build brand trust and deliver on your vision. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X and LinkedIn. Published 08/25.