TRINITY CYBER

Preemptive Cybersecurity for Financial Institutions

Solutions Brief

NOVEMBER 2025

240.654.1451
info@trinitycyber.com

© Trinity Cyber Inc. 2025. All Rights Reserved | 16701 Melford Blvd #300, Bowie, MD 20715

TRINITY CYBER

> "Community bankers agreed that the cyber-threat risk is enormous; some said existential."
>
> CSBS Community Banking Survey, Community Banking in the 21st Century

- **For the past five years (2021-2025) cybersecurity risk has remained the #1 concern of community financial institutions,** beyond credit risk, liquidity risk, staffing, and a wealth of other concerns, according to the Conference of State Bank Supervisors (CSBS).
- **AI-based threats are overwhelming even the largest financial institutions.** Attackers increasingly automate reconnaissance, produce tailored attacks at scale, clone voices and faces, and mutate malware in ways that circumvent conventional defenses.
- **Smaller financial institutions, including community banks, credit unions, savings and loans, and specialty lenders, face a distinct exposure profile:** concentrated dependencies on a few core processors and SaaS vendors, thin security staffing, and regulatory obligations that are resource intensive to operationalize.
- **Gartner projects that preemptive security will represent 50% of IT security spending by 2030.** Gartner advises moving from traditional detect-and-respond capabilities to preemptive controls that deny, deceive, and disrupt attackers.

The implication is clear: conventional detection and response approaches have failed.

Preemptive Security Benefits in Practice

Trinity Cyber delivers a superior security service edge (SSE) and zero trust network access (ZTNA) approach made possible by its real-time Full Content Inspection technology. Tailored to the needs of financial institutions that require strong threat protection and no periods of assumed trust, Trinity Cyber's FCI is the pioneer in preemptive security:

- **Employs a proven and differentiated detection approach** that protects over three million end users and 200 million network objects. FCI identifies threats using adversary behavior and context. Its active, inline preventive controls stop threats in protocols and files before they enter or exit your network and endpoints.
- **Protects your network and endpoints from threats, while enabling zero-trust application access.** Traditional SSE/ZTNA stacks typically allow or block whole sessions without inspecting payloads. They don't edit malware out of live traffic or remove malicious content in real time.
- **Enables business continuity.** FCI removes malicious objects inline, in real time without block pages or user friction. Malicious ransomware payloads are stripped, neutralizing exploit attempts and blunting credential-harvesting.
- **Lowers burden on financial institution IT staff.** IT gets time back, with less cybersecurity disruption and no alerts. Instead, Trinity Cyber cleans traffic in real time.

Trinity Cyber provides drop-in risk reduction that works with the tools financial institutions already have **and provides evidence that supports audits and answers regulator questions.**

© Trinity Cyber Inc. 2025. All Rights Reserved

TRINITY CYBER

Key Features

Zero Trust Network Access (Internet + Private Apps)
Connect users to the internet and private resources with strong endpoint protection. Trinity Cyber provides a practical VPN replacement with IdP/SSO/MFA integration.

Network Intrusion Prevention, Web Gateway, and Cloud Firewall
Trinity Cyber includes cloud firewall and web gateway functions for full visibility and control.

Full Session Search
Trinity Cyber provides full visibility and PCAP to quickly answer every day IT and security questions, such as:

- Why is a user having performance issues?
- Who's using an illicit Sharepoint instance?
- Do we have clandestine DoH/DoT or RDP usage?
- Where is legacy TLS in my environment?
- Which ISP path is dropping packets?

AI-Accelerated Threat Protection
Trinity Cyber uses AI to defend against today's AI-powered threats. Its AI models are built and operated in a secure enclave and engineered for microsecond -class identification. The result? Accelerated inline neutralization that enables real-time protection with near-zero false positives at global scale.

Why Community Financial Institutions Use Trinity Cyber

- **Drop in risk reduction:** Rapid deployment with security aligned to zero-trust principles.
- **End-user acceptance:** Transparent session sanitization keeps business moving.
- **Quiet, efficient operations:** Alertless preemptive remediation provides financial institutions clean traffic and evidence-rich visibility.
    - IdP/SSO/MFA integration uses what you already trust.
    - Interoperable with existing networking infrastructure and endpoint detection and response solutions.

Try Trinity Cyber in Your Network Environment

- **Join our 14-day pilot (up to 500 users):** Connect to private apps and the Internet; integrate with your IdP. You'll see first-hand how Trinity Cyber sanitizes objects and blocks callbacks with low latency.
- **Ask about our VPN buyback program.** Take advantage of our credit program when you switch to Trinity Cyber.

© Trinity Cyber Inc. 2025. All Rights Reserved