RADICL™
NEXT-GEN CYBERSECURITY-AS-A-SERVICE

US FEDERAL CREDIT UNION 1364 | CASE STUDY

From Reactive Recovery to Proactive Threat Dominance

Why U S Federal Credit Union Chose RADICL's Cybersecurity-as-a-Service (CSaaS) to Transform its Security Operations

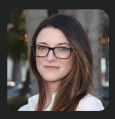
ABOUT U S FEDERAL CREDIT UNION

Headquartered in Northwest Indiana, U S #1364 Federal Credit Union is entrusted by local members with the safety and security of their financial assets and personal information. When Nicole Smith became President & CEO, she stepped into an organization that had recently navigated a cyber security incident and immediately prioritized strengthening its security posture.

Working closely with Steven Ruiz, Vice President of Information Technology and Security, and with the full support of the Board of Directors, she accelerated the usual evaluation process to address the situation with urgency. *"Given the circumstances, it was important to move faster than our typical timeline,"* Smith shared. *"Our focus was ensuring complete peace of mind that all member and employee data was secure and that every safeguard was fully in place."*

THE CYBERSECURITY CHALLENGE

> ***"My priority was to confirm that no vulnerabilities remained and that our member's information was fully secure against potential cyber threats."***



Nicole Smith
President & CEO
U S Federal Credit Union

For a member-owned credit union, the risk wasn't just technical — it was foundational. A breach can erode community trust and draw heightened National Credit Union Association (NCUA) scrutiny. Nicole recognized that in a rapidly advancing digital banking environment, traditional security measures were no longer sufficient. To protect the credit union's future, U S Federal needed a comprehensive and modern cyber security framework capable of anticipating emerging threats, safeguarding data and supporting long-term growth with confidence.

As with many credit unions of its size, U S Federal Credit Union's previous cybersecurity approach reflected traditional practices that were once standard but are no longer sufficient in today's digital banking environment.

Evolving Cybersecurity Standards

Prior to modernization efforts, U S Federal Credit Union's IT environment reflected common practices for smaller institutions, but it did not yet align with today's rapidly advancing cybersecurity frameworks. As threats have grown more sophisticated, the need for a formalized, measurable security standard became increasingly important.

Limited Visibility Across Tools

Like many institutions using multiple service providers, U S Federal Credit Union had fragmented visibility into its security environment. Alerts existed, but a modern, unified approach to threat monitoring and response was needed to streamline visibility, reduce gaps, and ensure faster action on emerging threats.

Legacy, Reactive Tools

U S Federal Credit Union's prior security tools and processes were consistent with what many credit unions historically used. However, the rapid shift in the threat landscape meant these legacy, reactive defenses were no longer sufficient. Moving toward a proactive, next-generation protection strategy became essential to reduce risk and strengthen resilience.

Limited Transparency Into Vendor Activities

Prior to restructuring, U S Federal had multiple external providers handling portions of IT and security. This made it challenging to maintain a complete, real-time picture of activity across systems. Improving transparency and consolidating oversight became a key priority to ensure the credit union could move confidently toward a more integrated and accountable security model.

THE RADICL EXPERIENCE

RADICL replaced piecemeal solutions delivered by multiple vendors with integrated Cybersecurity-as-a-Service (CSaaS). With RADICL, U S Federal now experiences and enjoys:

> ***"If you cannot afford to have robust security, you have no business being in business."***
>
> **- Nicole Smith**

Cybersecurity Governance Against NIST CSF

RADICL is expertly guiding and enabling ongoing compliance with the NIST Cybersecurity Framework (CSF). CSF provides an industry recognized collection of best practices for ensuring appropriate measures and controls are in place to reduce the risk of experiencing cybersecurity related incidents. Adherence with NIST CSF provides Nicole and the U S Federal Board of Directors assurance their MSP and internal IT team are working within a baseline cybersecurity standard to keep member data safe.

Proactive and Modern Threat Protection

RADICL has deployed best-in-class CrowdStrike EDR across endpoint and server infrastructure, optimally configuring it to ensure best-in-class proactive threat defense. RADICL is also driving proactive and risk aligned vulnerability management operations, ensuring avenues of attack are being constantly reduced. In addition, RADICL is reducing employee-related risks via ongoing security awareness training and phishing simulations.

Extensive and Deep Threat Hunting

RADICL is monitoring the broad IT environment for evidence of attack. Proprietary detection analytics run 24/7 looking for threat indicators across endpoint, identity, and network attack vectors. Military-grade "Deep Hunts" are executed on a weekly basis to see if a novel or internal threat has evaded detection and is lurking from within.

End-to-end Incident Response

RADICL has taken on full operational responsibility for the entire incident response process—from alert triage through full investigation to incident response and recovery, RADICL owns, executes, and drives the process. Nicole and the U S Federal board have assurance that if an incident were to occur, it would be expertly handled with clear vendor ownership.

Operational Transparency and Accountability

Nicole and the U S Federal team have direct access to the RADICL platform. They can see exactly what RADICL is doing and has done to keep them safe. Progress against NIST CSF compliance and vulnerability management, along with actions taken or needed by their MSP, is clear. Employee security awareness readiness or risk is also clear. Through RADICL transparency, accountability and trust are held.

BUSINESS IMPACT

"We're no longer just reacting — we know where we stand, we know what's next, and we have evidence to back it up."

Steven Ruiz
VP IT & Security
U S Federal Credit Union

This transformation, as Steven Ruiz describes, represents more than operational improvement - it's institutional confidence.

U S Federal now operates with enterprise-grade protection across all attack vectors through a single integrated platform rather than disparate point solutions.

"Your platform was eye-opening, just how RADICL set it up, it gave us different purviews into different sectors of our environment," Steven notes. *"This is what's going on in our environment. We didn't have that before."* The comprehensive visibility enables U S Federal Credit Union to walk into NCUA exams with real-time, evidence-backed security controls, dramatically reducing audit preparation time while ensuring sensitive member data remains secure.

Perhaps most importantly, RADICL has become Steven's benchmark for vendor partnerships: *"The partnership that we have with RADICL is my baseline for our other vendors. This is what I want."* This relationship standard reflects the accountability and transparency that traditional MDR providers couldn't deliver - continuous monitoring and proactive threat hunting that protects members while maintaining the operational efficiency needed to serve the community.

U S Federal Credit union now operates with confidence, knowing that member data is protected while maintaining the operational efficiency needed to serve their community.

"The out-of-box experience exceeded what I saw in the demo, which is uncommon. I have shared that feedback with my network, and during a CEO roundtable with over 100 credit union leaders, I was pleased to recommend RADICL."

Nicole Smith
President & CEO | U S Federal Credit Union