ECLYPSIUM

CASE STUDY_

First Financial Fights Cyberattacks by Securing Their Firmware

FIRST FINANCIAL
CREDIT ♦ UNION

LOCATION_	New Mexico
SIZE_	16 branches and over 85,000 members
SERVICES_	Full service credit union: checking, savings, loans, mortgages, business banking, financial education
ASSETS_	Over $800,000,000
BUSINESS NEED_	Risk management and FFIEC compliance
ECLYPSIUM SOLUTION_	Firmware security for endpoints. Plans in place for network device and server protections.

Credit unions are considered by many to be the backbone of our regional economies. They often predict regional futures and preserve impressive stories of economic turnarounds. First Financial Credit Union of New Mexico, for instance, has grown since 1937 from a small firm serving only the members of a regional Bell telephone utility, to a poster child of the impacts of the Ma Bell breakup of the eighties, to one of New Mexico's 8 largest credit unions. First Financial is now a market leader in the state, with assets over $800 million and serving more than 85,000 members across dozens of different New Mexico employers and agencies.

Because of their visibility and the way they reflect regional economic fortunes, credit unions are also powerful magnets for financially motivated cyber attacks and politically motivated disruption. At a March 2022 meeting of the National Credit Union Association (NCUA), immediately following the start of Russia-Ukraine hostilities, NCUA Chairman Todd Harper was direct in his warnings about these threats: **"I cannot stress this enough: All credit unions and vendors, regardless of size, are vulnerable to cyberattacks."** He also urged that "all parties within the system must maintain the highest level of alertness."

Steve Coffey, First Financial's VP of Information Technology, didn't really need the additional urging. His background in cybersecurity had already caused him to form a team whose tendency was to place First Financial ahead of emerging threats rather than behind them. Instead of responding to audit findings and deficit checklists, the team always asked pointed questions about new threat vectors and the likelihood of new attacks.

Coffey reported that firmware security was an area that had recently come into focus. "Our first questions on seeing new firmware-focused attacks were whether our existing tools had visibility and effectiveness in the sub-OS areas of our systems, where firmware lives. And then we needed to know how easy these attacks were to organize and execute."

His team's research revealed that No, there were significant visibility and protection gaps at the firmware level, and Yes, it wasn't just powerful nation-states doing the attacking. They quickly put together a set of requirements potential solutions would need to meet:

- Because firmware is everywhere, in all device types, the ideal solution would cover endpoints like the laptops used by execs and the desktop clients used in branches, as well as a variety of network devices and the on-prem servers the organization still maintains.
- The team needed a solution that could leverage a huge population of existing firmware profiles and details, across the widest possible set of vendors and devices.
- The solution would need to assess not just current firmware versions and integrity, but because firmware has grown increasingly complex and powerful, its security and operational configurations as well.
- Eventually the solution would need to cross organizational boundaries between security and operations teams, and they wanted one that could provide not only detective insight but also take protective and corrective actions, like firmware updating and configuration adjustment, if needed in the future.

In addition to these requirements, the team needed a solution that deployed rapidly and easily, and that wouldn't burden cybersecurity specialists and admins. As Wayne Davidson, one of Coffey's cybersecurity managers remarked, "The best tools are the ones that don't require a lot of lift to get going but still give you immediate insight."

While protection requirements for firmware are just now appearing in many cybersecurity regulations and standards, there was good guidance already in place from the Federal Financial Institutions Examination Council (FFIEC) regarding proper protection of firmware. The FFIEC IT security handbook from 2016 calls out detection of firmware vulnerabilities and firmware configuration management as key areas of focus. A more recent piece of FFIEC guidance, Authentication and Access to Financial Institution Services and Systems, published in 2021, cautions on the need to update and configure firmware in security devices – a particularly popular target since the Kaseya and Pulse Secure compromises of 2021. Resources like this provided guardrails for what First Financial's chosen solution would need to accomplish.

After evaluating multiple vendors, Coffey and Davidson chose Eclypsium to be First Financial's firmware security vendor in early 2022. Initial trials and rollouts have been a success and the team is pleased with the additional layer of protection provided – without excessive overhead – to laptops, desktops, and thin clients throughout the network.

"New attacks at the firmware level, like iLOBleed implants in servers and FinSpy bootkits in endpoints, are getting news exposure almost daily," says Coffey. "By deploying Eclypsium we're staying ahead of these low-level threats. And we're getting the right tools in place well before auditors ask for evidence of firmware protections, which can happen at any time given the increased threat levels facing credit unions."

Future expansions may include network device coverage and the use of Eclypsium to detect the firmware-based indicators of compromise (IOCs) that reveal ransomware activities invisible to EDR tools. As Davidson remarked, "Our goal is to have a layered solution from which we can extract more and more security value as we grow."