

No Blind Spots, No Surprises: How Global Credit Union Secures Acquisitions with Confidence

GLOBAL CREDIT UNION

AT A GLANCE

INDUSTRY

- Financial Services / Credit Union

ENVIRONMENT

- 2,100+ employees
- 11,000+ endpoints across IT and branch networks
- Multi-state and international footprint: Alaska, Arizona, California, Idaho, Washington
- U.S. Air Force bases in Alaska and Italy

CHALLENGE

- No visibility into devices connected at the port level
- Inherited unknown infrastructure across M&A targets
- Immovable Legal Day One deadlines requiring pre-integration insight

FORESCOUT 4D PLATFORM™

- Forescout Security Automation & Control Bundle:
 - eyeSight
 - eyeControl
 - eyeExtend

Financial services · Network visibility · M&A security

THE CHALLENGE

Global Credit Union (GCU) had a problem that most security teams can sympathize with... they didn't know everything that was on their network because of mergers and acquisitions (M&A). Before the pandemic, the Alaska-founded credit union operated primarily from physical branches with a centralized footprint. But rogue devices and unsecured ports across an expanding network were a real and growing concern.

"We had already experienced issues," says Dana Gonderzik, Director of Information Security. "We were also hearing more about threat actors using social engineering to get into organizations' buildings and actually plugging in devices to listen and capture information. We didn't want to be a victim of that, so we needed to act quickly."

As GCU accelerated an ambitious merger and acquisition strategy, that challenge became exponentially more complex. Each acquisition brought unknown infrastructure, forgotten systems, and inherited risk. And in M&A, time is never on your side.

"With Forescout, we don't have to have agents to identify anything. Through policies and configurations, we can secure acquired companies fast."

— Dana Gonderzik, Director, Information Security

THE SOLUTION

GCU deployed Forescout in 2019, drawn by one overriding requirement: speed. "It was the quickest and fastest deployment to get secure," Gonderzik explains. "We didn't have to have agents to identify anything. Through the policies and configurations, we could do this fast. And use agents if and when we wanted. We weren't forced down that road."

That agentless approach gave the security team immediate visibility across all 11,000+ endpoints without the weeks of agent deployment that competing solutions required. But the real game-changer came when GCU applied Forescout to its M&A process.

The team built what they call an "M&A box" — a portable deployment kit with Forescout at its core. When an acquisition target is identified, the box is shipped to the target organization with simple setup instructions. A few firewall rules, a VPN connection back to GCU's environment, and a configured switch port are all it takes.

USE CASES

- Network access control and port-level security
- M&A pre-integration asset discovery
- Legacy OS and shadow IT detection
- Agentless endpoint visibility

RESULTS

- Full network visibility within days of deployment
- Hidden risks uncovered before every Legal Day One
- Legacy OS and shadow IT exposed in acquired networks
- Proactive risk management replacing reactive response

Forescout can be operational in new acquisitions within a few days – giving us the network visibility we need to make critical keep-or-replace decisions before we inherit any risk.

— Chase Albers,
Information Security Architect,
Global Credit Union

“It’s pretty plug-and-play,” says Information Security Architect Chase Albers. “Usually, it can be done within a few days for their IT team to plug it in and do what they need to do.” Within days – not weeks – Global Credit Union has complete network visibility into a network it doesn’t yet control.

THE RESULTS

That pre-integration visibility has proven invaluable. In M&A, Legal Day One – the moment ownership legally transfers – is an immovable deadline. Arriving at that date unprepared means inheriting unknown risks into a live production environment. Forescout changes that equation entirely.

“We were able to utilize Forescout to determine some of the things on an M&A network that the acquired team had forgotten about that were quite risky,” Gonderzik says. “We could take care of them before there was risk to GCU’s network.” The most striking example: Windows 7 machines running in an acquisition target’s environment that the target organization itself didn’t know existed.

But the discoveries don’t stop at legacy operating systems. Forescout surfaces shadow IT, forgotten service contracts, and hidden vulnerabilities that even thorough due diligence misses. “There have been others,” Gonderzik notes. “Different vulnerabilities we’ve removed, different services we’ve identified in contracts that we didn’t know about—that we could handle proactively versus reactively.”

That shift – from reactive to proactive – is perhaps the most important outcome of all. Problems identified before Legal Day One are far easier and less expensive to resolve than those discovered after integration is complete.

LOOKING AHEAD

Global Credit Union continues to advance its Zero Trust journey, with Albers working to deepen trust-but-verify capabilities across its security stack. “Three years ago, we thought we were getting pretty close to what Zero Trust was,” he reflects. “Now we look forward and realize there’s more to do here – it’s just something we need to keep up with.”

As the credit union’s M&A-driven growth continues, Forescout remains central to its security architecture – not as a bottleneck, but as an enabler. Global Credit Union evaluates and selects target organizations based on their culture and mission fit, confident that whatever infrastructure they’re running, Forescout will reveal the true state of their network in days. Before Legal Day One. Every time.

About Forescout

For over 25 years, organizations and governments worldwide have trusted Forescout to secure their networks. From pioneering Network Access Control (NAC) to delivering Universal Zero Trust Network Access (UZTNA), Forescout leads the evolution of enterprise network security across IT, OT, IoT, and IoMT environments. The Forescout 4D Platform™ delivers comprehensive asset intelligence, continuous risk assessment, and dynamic control, over all managed and unmanaged assets, enhanced by the proprietary threat intelligence research of Vedere Labs. Leveraging agentic AI workflows with human-in-the-loop actions, Forescout continuously analyzes threats, orchestrates response, and integrates seamlessly with 180+ security and IT products.



Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at [Forescout.com](https://www.forescout.com)

©2026 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.
04_26_V09