

## Innovation Federal Credit Union: Connecting and Securing a Growing Hybrid Workforce



**Industry:**  
Financial Services

**Location:**  
Saskatchewan, Canada

**Organization:**  
520 employees, 28 locations

**Solution:**  
Cisco Secure Access

With over \$5.5 billion in managed assets, Innovation Federal Credit Union serves 67,000+ members across 28 locations throughout Canada. As a federally regulated organization with the opportunity to vastly scale its business, Innovation needed a more modern approach to enabling and securing its growing hybrid workforce, regardless of location or device.

Of the 400+ credit unions operating within Canada, Innovation Federal Credit Union (Innovation) is among only three that are federally regulated. This status allows Innovation to expand nationwide, opening locations anywhere within Canada and attracting top talent from across the country.

When Innovation transitioned from a provincially regulated business to a federally operating credit union, the opportunity for growth came with significant challenges:

- Protecting and enabling a growing remote workforce**  
A large portion of Innovation's workforce was already remote, with numbers set to rise. However, due to a mix of connection methods and cumbersome security processes, remote workers already faced persistent performance and latency issues, while IT and support teams were strained by constant requests for assistance. Additionally, once users left the physical office, they were no longer protected by perimeter defenses, creating a gap in protection for remote workers and raising serious security concerns.
- Complying with federal security regulations**  
Securing Innovation's hybrid workforce is essential to meeting compliance rules from federal regulators like the Office of the Superintendent of Financial Institutions (OSFI). But with the limitations of their existing cybersecurity approach, scaling Innovation's remote workforce would significantly increase the company's vulnerability and exposure to cyber threats.

"With ZTNA, our hybrid workforce automatically connects to any resource, from any location and device – without having to take extra steps. The user experience is seamless and transparent. That's exactly the security strategy we needed."



– Shawn Spurko,  
Vice President Information and Cyber Security,  
Innovation Federal Credit Union

## Seamless, Transparent, Secure Access – from Anything to Anywhere

Relying on a Managed Services provider for most of their networking security needs, Shawn Spurko, Vice President Information and Cyber Security for Innovation, sought a modern remote access solution. “My immediate priority was implementing zero trust capabilities to provide consistent security controls and seamless connectivity to all employees, regardless of their location or device.”

Innovation selected Cisco Secure Access, a natural move since they were already using Cisco Umbrella DNS. “The platform includes the same Umbrella DNS features we were using plus additional security controls we needed, like Zero Trust Network Access (ZTNA),” explains Spurko.

He valued the granular control over traffic routing and security policies. “With ZTNA, the remote end user experience is seamless and transparent.” ZTNA dynamically authenticates users and applies security and connection policies based on their location, device, and access needs. “Our hybrid workforce can connect to any resource, from any location and device – without having to take extra steps. That’s exactly the security strategy we needed.”

## A Phased Approach to Strengthening Cybersecurity

Today, all 520 employees are protected by Secure Access – Internet Access (SIA) and Secure Access – Private Access (SPA). Innovation rolled out DNS and ZTNA to every employee and plans to deploy all the platform’s capabilities.

- **Transitioning from Umbrella DNS:** Every user previously protected by Umbrella DNS is now covered by Secure Access DNS filtering. “The transition was extremely easy and smooth,” notes Spurko.

- **Infusing zero trust principles:** Rolling out ZTNA to all employees took the IT group just a few days and required only minutes for end-user enrollment. “The connection process is completely transparent, no matter where the users and resources are located.”
- **Delivering VPN via the Cloud:** While all users rely on ZTNA, Innovation is testing the Secure Access VPN-as-a-Service (VPNaaS) to ensure the functionality is available when needed to improve IT management capabilities. “It’s built right into the solution, requiring no extra work on our part,” reports Spurko.
- **Securing mobile devices:** Innovation built a new Corporate Device Management solution that includes Secure Access (DNS Security, VPNaaS and ZTNA) as a backbone for mobile security and connectivity for both iPhones and Androids. The company completed the process of migrating users to the new corporate mobile devices within a week.
- **Advanced features:** Innovation just completed rolling out Secure Access advanced features to all employees including decryption of traffic, the IDS client, the Data Loss Prevention (DLP) options, and the Secure Web Gateway (SWG).

In addition to Secure Access, Innovation is utilizing Cisco Firepower Firewalls for advanced security, threat intelligence, and intrusion prevention. Because Firepower and Secure Access share foundational technology, Spurko says making changes or adjustments – for example, to their Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) – is straightforward. “This unified approach to cybersecurity ensures cohesive protection across our on-premises and remote access solutions. If a change works in Firepower, we can quickly and easily apply the same profile that’s already built into Secure Access.”

## Stronger Security, Seamless Connectivity, and Scalable Growth

Innovation has achieved significant outcomes using Secure Access, from improving the user experience and productivity to complying with federal rules while expanding the business nationwide.

### Scaling protection and visibility

Nearly half of Innovation's employees work remotely or travel frequently. Spurko notes, "With Secure Access, we're providing 40% of our entire workforce with 24/7 security protections they never had before." Innovation has fortified its risk posture, reducing the likelihood of cyberattacks and non-compliance penalties. Additionally, with data loss prevention capabilities, they can analyze data in-line to monitor how sensitive data is being used.

### Improving the user experience

Seamless security and connectivity have significantly improved the user experience. "Our remote workers don't have to launch multiple software clients that use different sign-on processes or worry about latency impacting productivity," says Spurko. "They simply connect through a single client and go - the authentication and connection processes are all handled transparently."

### Increasing efficiency

Using the Secure Access Machine Tunnel VPN feature vs. their previous VPN solution, Innovation estimates it is saving users and IT staff approximately 11.5 hours per month previously spent on resetting passwords, helping users locked out of the old VPN to regain access, and replacing expired keys for users who lost VPN access due to infrequent usage.

"With Secure Access, our users' computers are now always connected to the VPN through the Machine Tunnel, even when they don't realize it, which keeps the connection to

our domain controllers," explains Spurko. "Because the only traffic that goes over the Machine Tunnel is the traffic we need for management purposes, it doesn't slow down the user's internet connection."

### Simplifying IT operations

With a single console and centralized policy creation, the IT and support teams are responding faster to user needs. Spurko reports, "Where it once took weeks to complete remote user requests for access to internal resources, it now takes only a day or two." IT and support have also decreased time spent troubleshooting user connectivity issues, enabling them to focus on adding value to the business, like testing and deploying new security capabilities.

### Meeting federal regulations

Innovation has the security, automation and visibility in place to meet federal laws. In compliance with OSFI, Innovation conducts an annual cybersecurity assessment, identifying vulnerabilities it can address to increase their cybersecurity maturity. "We have addressed many of the gaps with Secure Access, both in terms of its capabilities and its ability to scale coverage across our hybrid workforce."

## Continuous Innovation for a More Secure Future

Innovation plans to expand the applications made available through ZTNA. "Cisco continues to roll out new functionality that allows us to do more with ZTNA—capabilities that weren't even an option two months ago." That's one of the things Spurko values most about Secure Access, how quickly the platform is evolving. "New features are added weekly, and we're committed to keeping up with the technology so we can continuously modernize and strengthen how we enable and protect our hybrid workforce."