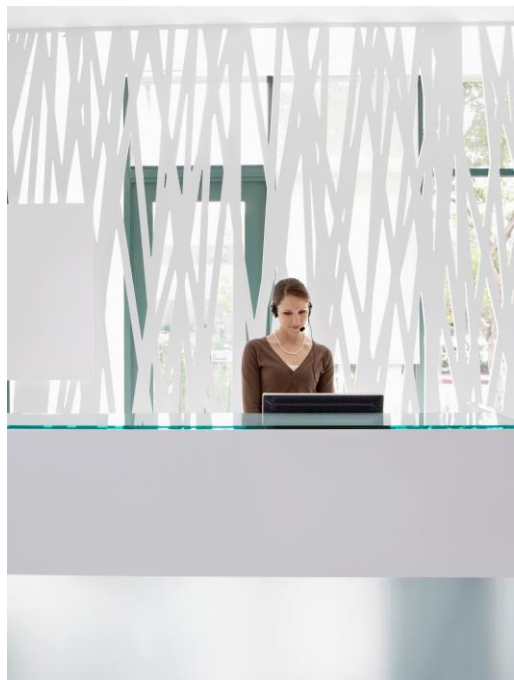


Lumen and ThreatX team up to give SELCO Community Credit Union's IT Team the watchdog it was looking for



The Customer

SELCO Community Credit Union

Located in Springfield, Oregon, SELCO is one of Oregon's largest and most longstanding credit unions.

It is a member-owned, not-for-profit financial cooperative offering a full range of banking and financial services, including personal and business banking, personal and commercial lending, financial planning and investment services, and a range of insurance products for individuals and businesses.

With a current asset size of \$2.5 billion, SELCO has 143,000 members and 14 branches serving 27 Oregon counties.

The Challenge

Since the start of the pandemic, every financial institution has seen an uptick in attempted cyberattacks — from brute force to DDoS to credential stuffing. As part of its proactive and aggressive commitment to data security, SELCO Community Credit Union enlisted the services of Lumen and ThreatX to ensure that if a threat were ever to present itself, SELCO's members and their information would remain secure. "We were looking for outside expertise and a way to continue delivering best-in-class services without downtime, and without risk," said Steve Liu, SELCO's Director of Information Technology.

Juggling Excel spreadsheets

The SELCO IT team was working nights and weekends due to the manual and time-consuming process of responding to possible suspicious behavior using its previous security solution.

If the team identified unusual user behavior that could potentially be malicious, they'd pull IP addresses out of the suspected database queries, put them into Excel spreadsheets, remove any duplicates, and then correlate the IP addresses with other information. For instance, multiple logins with different usernames from the same IP address would be something to block. Ultimately, they would need to create rules for each identified IP address in their security solution. Unfortunately, even this detailed and time-consuming process couldn't account for ISPs that mask their customer IPs behind a single IP.

Challenge

Continue delivering best-in-class member services without downtime, and without risk

Solution

ThreatX Web Application and API Protection platform deployed via Lumen Application Delivery Solutions

Results

- ThreatX allows the SELCO IT team to protect member data without spending excessive time manually creating and managing rules.
- SELCO deployed ThreatX directly on the Lumen Edge Application Delivery platform, thus avoiding advanced configuration work.
- With ThreatX's attacker-based analysis, SELCO blocks suspicious activity without affecting legitimate traffic.
- SELCO was up and running on ThreatX via Lumen Application Delivery Solutions within an hour, and saw results just as quickly.

The Solution

A reliable WAF and API protection solution easily deployed on the Lumen edge

In its quest to provide services to their members without downtime or risk, SELCO investigated several web application firewall (WAF) vendors and bot management services. As part of that investigation, they reached out to Lumen as their ISP for recommendations. The Lumen team introduced SELCO to ThreatX, one of the top security vendors within the Lumen application ecosystem.

In one of the very first calls between SELCO and ThreatX, the ThreatX team proposed deploying their Web Application and API Protection (WAAP) solution right then and there to give SELCO a taste of what it could do. Within an hour, SELCO was up and running on the ThreatX platform. "It was pretty incredible," Liu remembered. "That spoke volumes to us about the responsiveness, the ease of integration, and just how quickly we could get it done."

An extension of the SELCO team

After evaluating other solutions, SELCO determined they couldn't match the level of preventative measures and efficiency they had found with ThreatX on Lumen. By that point, the SELCO team had developed great working relationships with the ThreatX SOC team that would have been hard to walk away from. "We had an amazing relationship with the ThreatX SOC. Individuals in the SOC would contact us, reach out to us. They felt like an extension of our team," said Liu.

"We quickly realized that ThreatX was the solution for us. Not just because of what the product could do and its fit for our systems, but also the dynamic, working relationship we had between my network team, myself, and key people at Lumen and ThreatX."

The Benefits

Restored balance on the team

"ThreatX on Lumen has been a game changer for my team and me," Liu said, "and has provided an additional layer of security for our members. We were all taking turns working evenings and weekends, and the need for that stopped."

Liu said that, early on, his team had to unlearn some of its ingrained methods of dealing with suspicious behavior and just let the ThreatX system do its thing. With ThreatX's behavior-based, rather than signature-based, analysis, it was actively identifying and blocking suspicious users without the need to manually create rules.

Liu said that his team has its balance back. "We don't have to be watching it all the time. It doesn't occur to me to check it over the weekend. As a small and specialized team, we don't have the ability to just watch out for potential threats or suspicious activity."

“ It wasn't the typical vendor assertion of, this is what we do, take it or leave it. The team is always willing to work with us and listen to our ideas to improve the product and the experience for other credit unions. In fact, we've seen that come to fruition in dashboard improvements that originated with us. We really feel like our voice is being heard.”

-- Steve Liu, Director of IT,
SELCO Community Credit Union



Keeping member services up and running

ThreatX monitors and tracks user behavior, looking for suspicious patterns over time rather than simply identifying attack signatures, such as suspect IP addresses. For this reason, the results are much more accurate than those generated by a legacy WAF — and much less likely to block legitimate traffic.

Fast time to value

With ThreatX's agentless deployment and integration within the Lumen edge, SELCO was up and running on the platform within an hour, and seeing results just as quickly. In addition, ThreatX consolidates data on multiple attack types — including traditional OWASP attacks, bots and malicious automation, DDoS mitigation, and API-specific threats. SELCO has a clear picture of their risk quickly, without spending time chasing down results from multiple solutions.

Realizing what's possible

Working with Lumen and ThreatX creates future opportunities as well. Liu noted, "It wasn't the typical vendor assertion of, this is what we do, take it or leave it. The team is always willing to work with us and listen to our ideas to improve the product and the experience for other credit unions. In fact, we've seen that come to fruition in dashboard improvements that originated with us. We really feel like our voice is being heard."

“ As a small and specialized team, we don't have the ability to just watch out for potential threats or suspicious activity. Using ThreatX on Lumen has been a game changer for my team and me, and has provided an additional layer of security for our members.”

-- Steve Liu, Director of IT,
SELCO Community Credit Union

