South Ayrshire Council uses Egress Prevent and Defend to enhance security awareness, cut costs, and remove complexity

🏛 Local government | 🌐 Scotland, UK | 🏷 Egress Prevent, Defend

The challenge

As one of 32 councils in Scotland, South Ayrshire Council provides services to the citizens, residents and businesses that call Ayrshire home. And like other government agencies, South Ayrshire Council regularly deals with sensitive personal and financial information.

The Council's initial solution for ensuring secure communications was to secure a network completely separate from its corporate network. "To handle secure transactions and communication, we had a "secure enclave" of about 250 machines running our public service network services. But prior to our existing ICT Team's commitment to change, the corporate network didn't receive the same level of attention to security," said Anne Yeo, Senior ICT Security Analyst at South Ayrshire Council.

"I believe we were the only organization in Scotland that approached it like this; all other local authorities ran everything through their corporate networks. It became increasingly challenging because the people who used the secure network to communicate with other local authorities had to have two separate devices, logins, and email addresses. Maintaining and upgrading these devices

was expensive — even though it was a relatively small network compared to our larger corporate network, there was a lot of expenditure associated with servicing that for 300 people."

Additionally, the Council's ICT team wanted to change how the organization handled security, increasing user awareness. "We purchased an email phishing simulation tool and started running simulations. We had some initial success but often found that people shared information about the simulation. When we ran simulations, about half the people knew it was a simulation before they opened the email, which skewed our results. We could tell some people learned to slow down and pay closer attention to the email, but many people didn't change their behavior. We realized we needed something else to help empower our employees to make informed email decisions," Yeo said.

The Council's data governance team also had its own security concerns, namely, preventing accidental data breaches. "Our information governance and privacy are handled by a separate office outside the ICT team — and our data governance team was very conscious about needing a product that provided protection against people mistakenly sending information out. Previously, they had no idea how often data breaches happened due to internal human errors. We know that data breaches are historically underreported — people are embarrassed and don't want to get into trouble for a mistake they've made that could've led to a potentially bad situation," she explained.

> ❝
> We also wanted to replace the training we'd been doing via our phishing simulations with something that would truly impact user behavior — and we determined that Egress Prevent and Egress Defend used together would give us the perfect combination of user education and autonomy.
>
> Anne Yeo, Senior ICT Security Analyst, South Ayrshire Council

The solution

South Ayrshire Council's ICT team reviewed its security options and looked closely at two Egress solutions: Egress Prevent to mitigate against outbound data loss and Egress Defend to protect against inbound phishing threats. "We knew we needed to move away from the security enclave and secure our whole corporate network. We began looking for alternatives to support this transition, and Egress Prevent had already come to our attention when we'd been looking for solutions to protect our employees who needed to share highly sensitive information with external organizations. And my manager, Stewart McCall, saw Egress Defend in a call and thought its banners and notifications would help our staff," said Yeo.

"We also wanted to replace the training we'd been doing via our phishing simulations with something that would truly impact user behavior — and we determined that the real-time teachable moments from Egress Prevent and

Egress Defend used together would give us the perfect combination of user education and autonomy."

Adoption across the organization went smoothly. "People were willing to accept Egress. There were initial concerns about how challenging it would be to use and how it would impact sending emails, but people have found it straightforward to use as part of their daily work. And from a management standpoint, Defend is easy for the ICT team to administer and maintain," said Yeo.

User feedback on Egress has been overwhelmingly positive. "We want to find the balance between introducing friction into our employee's daily routines and reducing risk. One of the key things we've done is to completely block any email links that Defend finds suspicious. We found that some people were still clicking through links, even though Defend displayed a red banner that indicated that the email was almost certainly phishing. Defend allows us to ensure that users cannot click through those links," she said.

The results

Egress has boosted the Council's security across the organization while reducing complexity and costs. "We have mandated requirements to provide a certain level of security for our users who are accessing and sharing sensitive information," Yeo said. "But our security enclave approach came with significant complexity and costs. By bringing our corporate network up to a higher security standard with Egress, the whole organization benefits. And by removing the costs associated with maintaining a security enclave, we could redirect the budget to cover security for the entire organization."

Egress has also helped the Council's employees become more security conscious. "We do annual training to meet our compliance requirements and count on Egress Defend and Prevent to help shift user behavior. More than 1,000 users across our network use Egress, including the people in job roles that share sensitive personal or financial data with external clients — and the number of times users alert us to potentially suspicious emails has increased," she said. "And Egress has helped identify situations that our data governance team needs to look at more closely. Egress' analytics lets us see which threats are being blocked and which employees need additional information and training, allowing our data governance team to follow up with people directly. We've seen signs that things are getting better."

Egress has allowed South Ayrshire Council to show other Councils and partner organizations that it takes data security seriously. "Egress has allowed us to demonstrate to peers that our network security has changed and improved," Yeo concluded.

"

By bringing our corporate network up to a higher security standard with improvements that include Egress, the whole organization benefits. And by removing the costs associated with maintaining a security enclave, we were able to redirect the budget to cover security for the entire organization.

Anne Yeo, Senior ICT Security Analyst, South Ayrshire Council

www.egress.com