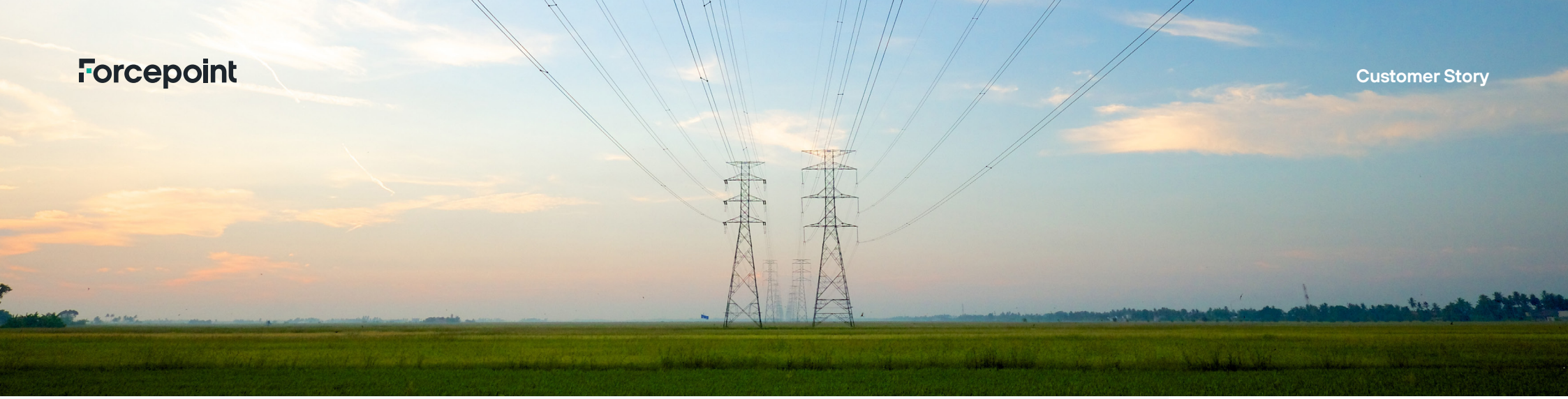

Irish Utility ESB Secures Its Digital Transformation Journey with Forcepoint

Ireland's national power company is protecting its cloud-driven technology strategy with the help of Forcepoint Edge Advantage.

Ireland's Electricity Supply Board relies on the internet and the cloud as mission-critical tools for the delivery of its critical infrastructure services to more than 1 million customers. After a long history of depending upon Forcepoint Web Security to secure its internet use, ESB upgraded to Forcepoint Edge Advantage as the cybersecurity foundation for the next phase of its SASE-protected digital transformation.

CUSTOMER PROFILE:
State-run utility providing power via energy generation, transmission, and distribution

INDUSTRY:
Energy

HQ COUNTRY:
Ireland

PRODUCT:
Forcepoint Edge Advantage

Ireland's Electricity Supply Board (ESB) is a diversified, vertically integrated utility supplying electricity to approximately 1.4 million customers and operating electricity networks in Ireland and Northern Ireland. ESB is a state-owned utility operating across the entire electricity market from power generation through transmission and distribution, and also has smaller stakes in natural gas distribution, networking and telecommunications, and electric vehicle public charging infrastructure.

ESB is a long-term Forcepoint customer, relying on Forcepoint Web Security to help protect its employees and the data they work with to maintain critical infrastructure, deliver power, and provide customer service. The utility operates multiple power stations in both Ireland and the UK, as well as the electricity grid in Northern Ireland—critical infrastructure that must be safeguarded against the increasing threat of advanced, malicious cyberattacks.

Effective protection against these threats requires flexible solutions that can be adapted to unique industrial contexts and challenges, while being strong enough to keep out even the most persistent or advanced adversary. As part of its digital transformation in recent years, ESB has sought the right cybersecurity approach to accompany its pivot towards cloud-native, SaaS-based solutions across its IT stack, said Chris Madden, ESB Cybersecurity Engineering Lead.

When it came time to renew with Forcepoint, ESB decided to migrate its Web Security from on-premises to a cloud-based implementation to better align with its increased use of cloud apps and platforms like Microsoft Office 365, Salesforce, and SAP HANA.

"Starting a few years ago, it became increasingly clear that our security infrastructure wasn't developed enough to get to where ESB wanted to go as an operator of essential services. "What we wanted was a market-leading provider of proxy services that were highly available and highly scalable, which met our technical and pricing needs, and which gave us the option of additional feature sets we could turn on as required in alignment with our digital strategy," Madden said.

ESB and Forcepoint mapped out a cybersecurity strategy that would begin with the migration of Web Security to a cloud-based deployment of Secure Web Gateway (SWG) and build over time toward a comprehensive, converged, SASE framework for securing the network edge and cloud access.

Phasing in SASE security solutions with the right vendor

In selecting a long-term cybersecurity partner for such an ambitious agenda, ESB wanted a vendor capable of helping it achieve several key strategic IT goals, Madden said. These included:

- → Reducing IT and cybersecurity complexity and improving operational efficiency.
- → Increasing capabilities for supporting and securing remote workers.
- → Building a strong relationship with a long-term strategic security partner with a wide-reaching portfolio strong in SaaS support and SASE solutions.
- → Adopting a phased approach to the rollout of transformational technologies as part of a five-year plan for growth and expansion.
- → Leveraging existing strategic technology partners such as Microsoft.

Challenges

Reducing IT and cybersecurity complexity and improving operational efficiency.

Increasing capabilities for supporting and securing remote workers.

Securing increased use of cloud applications and services.

Providing a SASE-based technology and cybersecurity strategy roadmap.

Approach

Deploy Forcepoint Edge Advantage's SWG and CASB as first part of a phased introduction of SASE cybersecurity solutions.

In addition to this list of strategic goals, ESB is extremely selective about which vendors it works with, Madden said.

"One particular thing that's very important for ESB is the client-vendor relationship. We've always had a very good relationship with Forcepoint, and we've always felt Forcepoint treated us as a valued customer. In all of our interactions, we've worked really well with our Country Manager and Forcepoint senior consultants, who are always greatly focused on meeting ESB's requirements and tailoring solutions to what we need," he said.

For the next phase of the partnership, ESB opted for a Forcepoint Edge Advantage license to both meet its immediate needs and to position itself for phasing in additional SASE cybersecurity protections over several years. Forcepoint Edge Advantage licenses SWG, Cloud Access Security Broker (CASB), Email Security, Intrusion Prevention Systems (IPS), and Next Generation Firewall (NGFW) with SD-WAN, plus Remote Browser Isolation (RBI) and Advanced Malware Detection (AMD) as optional add-ons. Further down the road, ESB will have the ability when required to add Forcepoint's data and user protection solutions with a comprehensive Forcepoint Advantage license.

"This suited us because the first thing we wanted to do was move Web Security to a scalable, cloud-delivered solution. Once we had that, our attention turns to what's coming down the road—that's more cloud, obviously. ESB have a cloud-first approach, and where it's not cloud-first, it's still likely to have cloud aspects, where we will only be increasing our consumption of cloud services over time," Madden said.

The Forcepoint Edge Advantage licensing model also means ESB will get new features as they're released at no additional cost and will have the ability to add unlimited users during the contract term, reducing total cost of ownership.

Forcepoint CASB gives ESB access to more of the cloud, safely

After deploying SWG, ESB began spinning up Forcepoint CASB to gain more visibility into and control over cloud apps used by employees, while still freeing people up to securely access the tools they need to do their jobs.

Forcepoint CASB protects ESB's sanctioned cloud applications from data loss and accelerates the use of modern CRM systems such as Salesforce through better data and user security. The combination of CASB and SWG also ensures that even unsanctioned, or "Shadow IT" cloud applications can be secured without necessarily being blocked.

"Having the integration between Forcepoint SWG and Forcepoint CASB was a big plus for ESB. Because they're linked and managed through a single pane of glass, ESB gets all the information it needs in one place with visibility across the board," said Forcepoint Country Manager Brian Barry.

Ultimately, ESB's deployment of Forcepoint CASB allows its people to use more of the cloud with reduced risk—meaning employees are empowered to experiment with new cloud applications in a secure fashion, safely gaining access to new tools that can introduce efficiencies and otherwise improve the business.

The next stage of ESB's cybersecurity transformation will be to deploy more Forcepoint Edge Advantage technologies like NGFW with SD-WAN, Barry said. The full solution platform is now available for ESB to turn on as needed to support initiatives like bringing new branch offices online more quickly, securing remote workers, and the planned introduction of a new primary cloud database.

Going forward, ESB will also consider using Forcepoint solutions for its operational technology (OT) security needs in addition to its IT security. One of the primary challenges faced by critical infrastructure organizations is maintaining unified visibility throughout the IT and OT stack. Forcepoint is one of the few cybersecurity vendors with the proven ability and product portfolio to bridge that gap—for example, deploying Forcepoint NGFW and Forcepoint Data Guard to secure traffic flow above and below the industrial zone, allowing for visibility through the full IT/OT stack, enabling the secure movement of data between physically segregated IT and OT systems, and greatly reducing the risk of compromise on either side.

A new model of security for a new way of working

ESB has seen tangible benefits from its partnership with Forcepoint and expects more to come, Madden said.

"In the context of what we do—the generation, transmission, and distribution of electricity—the use of the internet in our employees' day-to-day work is in fact a critical service for us and for our customers. When we first engaged with Forcepoint, we wanted a highly available system because the previous proxy solution encountered outages about ten times per year," he said.

"We haven't had one outage specifically related to the proxy itself since we upgraded to a more robust solution in 2016."

> **"We haven't had one outage specifically related to the proxy itself since we upgraded to a more robust solution in 2016."**
>
> **CHRIS MADDEN,** ESB CYBERSECURITY ENGINEERING LEAD

Madden believes Forcepoint and ESB are strongly aligned on cybersecurity strategy going forward. That synchronicity, along with Forcepoint's technology roadmap and enterprise services, will continue to inform ESB's long-term planning, he said.

"Forcepoint solutions are very important to our planning," Madden said. "We want to have all of the good things that come from mobility and collaboration and the cloud, which means we need to look at a different model of security for how we're providing internet and cloud access and protecting the network. The traditional 'castle-and-moat' approach to security is obsolete.

"Today, the perimeter is wherever your people are accessing from globally—that's where the security lies. The security is in your identity, the security is in your device, the security is in the data itself. We want to map that approach across our organization."

Results

- Reduced monthly internet outages to zero.
- Provided control over and visibility into employee cloud usage.
- Established a foundation for deploying SASE network, cloud, and data security solutions to keep pace with five-year digital transformation schedule.

Forcepoint