Case Study

SGN

Innovative UK Utility Company Enhances Security and Reduces Complexity to Stay Ahead of Cyber Security Challenges While Embracing the Cloud

Challenge

- Reducing cyber security complexity
- Plugging every possible security gap
- Finding a long-term cyber security partner that embraced the cloud
- Improving business processes to enhance safety and customer satisfaction
- Securely enabling the mobile workforce

Solution

- Symantec Managed Security Services
- Symantec Security Operations Center
- Symantec Web Security Service
- Symantec Global Intelligence Network
- Symantec CloudSOC
- Symantec Email Security Services

Benefits

- Strategic, single-vendor security partnership has reduced complexity
- In-house security team can concentrate on higher order tasks
- Secure migration to, and operation in, the cloud
- Improved productivity for remote workers
- Increased and accelerated risk maturity
- Robust security posture has enhanced customer trust

Client Profile

Site: sgn.co.uk
Industry: Utilities
Headquarters: Horley, UK
Employees: 5,000+

Cyber security threats and risks are inherent in the utility industry. SGN is part of the UK's critical national infrastructure and so it follows that safety is key: "Anything that affects safety, whether of employees, customers or the general public, is significant to SGN," says Mo Ahddoud, Chief Information Security Officer for SGN. "And cyber security is certainly one form of risk that could impact the safety. We know, for example, that nation state actors are active within the UK utility sector and that reminds us just how important it is to meet the cyber security challenge."

Mo is responsible for cyber security at an organization that distributes gas to 5.9 million homes and commercial properties around the UK, and the company has been working closely with the UK government around the NIS Directive, new European legislation covering security network and information systems. The NIS Directive is the first EU-wide legislation addressing cyber security and providing legal measures to boost cyber security overall. "It considers the maturity of security controls that critical national infrastructure organizations have in place," says Mo. "It mandates the definition of a robust and mature model that integrates within the whole of the gas and electricity distribution chain."

Customer satisfaction sits just behind safety in SGN's priorities. "Customer satisfaction is actually one of the big measures that government uses to gauge our license agreement," says Mo. "So it has to be pivotal! Consumers rightly have high expectations around data protection, whether it's personal banking, TV streaming, or getting the gas that heats their homes. They need to trust our security."

A Partner for the Cloud Generation

"We've moved 25 percent of workloads into the cloud so far, increasing to 100 percent by the end of 2019," says Mo. But he is keen to point out that the cloud journey is not about arriving at a fixed point; rather, it's a change in mindset. The technology and business challenges and demands constantly evolve, creating a complex ecosystem. "Cloud service provider offerings are enhanced on a daily basis," says Mo. "Applications like Microsoft Office 365, SharePoint, and Slack are so easy to consume and have high uptake, but there's also complexity around how to manage and control that whilst allowing the organization the flexibility and agility it needs. With Symantec we can lock security into the design and then just move workloads into that environment. We have the visibility and the controls in place. It's raised our risk maturity very quickly."

Benefits (cont.)

- Enhanced user behaviour visibility has improved decision making around cyber controls
- Facilitation of SGN cloud adoption principles of agility, cost savings, and security
- Better business engagement due to visibility of shadow IT

"For our security strategy, visibility of your environment is key because it means visibility of user behaviors. You can then make informed decision about what your controls need to be."

– Mo Ahddoud, Chief Information Security Officer, SGN

Mo recognizes that some in the industry are still very cloud cautious, with reservations about what type of data is put into the cloud and how it's managed. "I think you just have to remain very cognizant of the fact that you still own that data," says Mo. "The usual checks and balances don't just go away. It can be complex working with different providers, with different levels of assurance." SGN has had a strategic partnership with Symantec for some years, which was important in moving to the cloud. "We wanted a partner that really understood our business journey and really bought into that story; that's Symantec. It's fair to say that some vendors simply didn't have the foresight to understand the benefits of cloud services."

Workforce Transformation

Migration to cloud apps is an important part of SGN's organizational transformation, enhancing mobile productivity. Wherever possible the company is migrating to SaaS and enabling the mobile workforce, whether providing realtime mapping integrated with traffic flows, or optimizing gas incident workflows. "Our field workforce historically used laptops, but now uses tablets and we'll be moving some applications onto smart phones," says Mo. "It's a new opportunity to optimize our operations."

The SGN cloud program focuses on supporting operational, day-to-day work—providing applications and services at any time in any place with an impressive ease of use. "That's what's going to improve productivity for our teams in the field, and subsequently result in a better customer experience and higher satisfaction," says Mo. "So the way SGN designs and manages those applications and our cloud strategy is critical."

Like many utility companies, SGN is under ever-increasing pressure to reduce costs; the company also needs to investigate new ways of working and create innovation to build and diversify the business. "Cloud is playing a part in reducing the operational costs of our business and also as a starter for exploring potential new revenue streams," says Mo. "In order to support that kind of thinking and action you need an agile and, frankly, a more productive environment. The key principles for our cloud journey are agility, cost savings, and security. And security has been fundamental for the business case."

The Simplicity—and Effectiveness—of an Integrated Security Ecosystem

SGN is committed to reducing the complexity of security, as there are many point solutions on the market. "Developing a security partner approach with Symantec—integrating the Security Operations Center, Managed

Security Services, and more—created a central place to correlate our information," says Mo. It also enabled SGN to take advantage of the Symantec Global Intelligence Network, the world's largest civilian threat intelligence database. "The integrated threat intelligence network might see threats in Kuala Lumpur in the early hours of the morning, then update all of their environments to protect against that vulnerability," says Mo. "It really changes your security posture. It's very fast and very powerful."

"Rather than being bogged down and fending off constant low-level threats, my small team can concentrate on mapping between business risks and integrating that into the Symantec SOC and MSS."

– Mo Ahddoud, Chief Information Security Officer, SGN

The more threats Symantec manages the more Mo's team can focus on handling unique scenarios within the organization. "Rather than being bogged down and fending off constant low-level threats, my small team can concentrate on mapping between business risks and integrating that into the Symantec SOC and MSS," says Mo.

Symantec MSS also provides an optimized set of defined rules based on the experience and threat intelligence of Symantec globally. "The MSS is really important and has helped us accelerate our maturity," says Mo. "Symantec correlates a host of alerts from different log sources and provides understanding, whether it's seen that risk from an alert in the global threat portfolio, or maybe we've defined a response playbook that runs within the organization."

This breadth of vigilance is at the heart of SGN security. "When you consider all our connectivity—applications, cloud services, Internet of Things (IoT), and more—attackers have a wide spectrum of options. So we focus horizontally against all types of threats across all assets and devices. It's important always to be asking: What's highly critical? What would the impact be? Then ensure you have the security and agility to respond."

"With Symantec we can lock security into the design and then just move workloads into that environment. We have the visibility and the controls in place. It's raised our risk maturity very quickly."

– Mo Ahddoud, Chief Information Security Officer, SGN

Visibility as a Security Enabler

SGN wanted visibility into user behavior so it could make better-informed decisions about what controls to put in place—a key to the company's overall security strategy. By integrating the security suite with Symantec CloudSOC, Symantec's leading cloud access security broker (CASB), SGN got the visibility it was after. "For our security strategy, visibility of your environment is key because it means visibility of user behaviors," says Mo. "You can then make informed decision about what your controls need to be." Mo explains that historically SGN hasn't had this visibility but that Symantec CloudSOC is a very powerful business tool. For example, SGN now has visibility around shadow IT. "The visibility provided by CASB gives us control but it also gives the opportunity to engage with the business, to understand the need and maybe even use the insight to demonstrate and build a business case to fund the activity and bring it out of the shadows."

To protect email and web traffic and all their Microsoft Office 365 applications, SGN has turned to Symantec Email Security Services and Symantec Web Security Services, creating a culture where well educated and vigilant users are supported by robust technical controls. "I think the statistics say that over 95 percent of threats come through emails," says Mo. "So, for us, it's fundamental that we need to protect email because it remains a primary operation mechanism for our business. We've seen a very strong stance against malware from Symantec; the amount and type that's stopped." These Symantec services have also enabled Mo to provide a comprehensive picture of the threat landscape to the leadership team: "They now understand the situation much better, and they're impressed with the security capabilities we now have."

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-SRC-SGN-CS100 June 3, 2020